# 18-397-cv

IN THE

# United States Court of Appeals

FOR THE SECOND CIRCUIT

STUART FORCE, individually and as Administrator on behalf of the Estate of TAYLOR FORCE, ROBBI FORCE, KRISTIN ANN FORCE, ABRAHAM RON FRAENKEL, individually and as Administrator on behalf of the Estate of YAAKOV NAFTALI FRAENKEL, and as the natural and legal guardian of minor plaintiffs A.H.H.F, A.L.F, N.E.F, N.S.F, and S.R.F, A.H.H.F, A.L.F., N.E.F., N.S.F., S.R.F., RACHEL DEVORA SPRECHER FRAENKEL, individually and as Administrator on behalf of the Estate of YAAKOV NAFTALI FRAENKEL and as the natural and legal guardian of minor plaintiffs A.H.H.F, A.L.F, N.E.F, N.S.F, and S.R.F, TZVI AMITAY FRAENKEL, SHMUEL ELIMELECH BRAUN, individually and as Administrator on behalf of the Estate of CHAYA ZISSEL BRAUN, CHANA BRAUN, individually and as Administrator on behalf of the Estate of CHAYA ZISSEL BRAUN, SHIMSHON SAM HALPERIN, SARA HALPERIN, MURRAY BRAUN, ESTHER BRAUN, MICAH LAKIN AVNI, individually, and as Joint Administrator on behalf of the

*(Caption Continued on the Reverse)*

*On Appeal from the United States District Court*
*for the Eastern District of New York*

## BRIEF AND SPECIAL APPENDIX FOR PLAINTIFFS-APPELLANTS

Robert J. Tolchin
Meir Katz
THE BERKMAN LAW OFFICE, LLC
*Attorneys for Plaintiffs-Appellants*
111 Livingston Street, Suite 1928
Brooklyn, New York 11201
718-855-3627

Estate of RICHARD LAKIN, MAYA LAKIN, individually, and as Joint Administrator on behalf of the Estate of RICHARD LAKIN, MENACHEM MENDEL RIVKIN, individually, and as the natural and legal guardian of minor plaintiffs S.S.R., M.M.R., R.M.R., S.Z.R., BRACHA RIVKIN, individually, and as the natural and legal guardian of minor plaintiffs S.S.R., M.M.R., R.M.R., and S.Z.R., S.S.R., M.M.R., R.M.R., S.Z.R.,

*Plaintiffs-Appellants,*

*v.*

FACEBOOK, INC.,

*Defendant-Appellee.*

## Table of Contents

## Table of Authorities

### Cases

**Statutes, Regulations, and Rules**

**Israeli Authority**



**Other Authority**

# BRIEF FOR PLAINTIFFS-APPELLANTS

## JURISDICTIONAL STATEMENT

Plaintiffs commenced this action in the S.D.N.Y. against Defendant Facebook, Inc. (4-5[*]). On consent, it was transferred to the E.D.N.Y. (6). The district court (Garaufis, *J.*) dismissed the complaint "without prejudice" and issued judgment on May 18, 2017. (187-216). Plaintiffs timely moved under Rule 59(e) for reconsideration. The district court denied their motion by order entered January 18, 2018. (408-32). Plaintiffs timely noticed their appeal on February 8, 2018. (433-34).

The district court had subject matter jurisdiction under 28 U.S.C. 1331 and 18 U.S.C. 2333. Because this appeal follows final judgment of the district court, this Court has jurisdiction under 28 U.S.C. 1291.

## ISSUES PRESENTED

1. Whether the Anti-Terrorism Act, 18 U.S.C. 2331, *et seq.*, as amended ("ATA"), subjects Facebook to liability for supporting terrorism?

2. Does 47 U.S.C. 230(c) apply extraterritorially despite the lack of any indication that Congress intended extraterritorial application?

---

[*] Parenthetical page citations reference the Joint Appendix. "SPA" references the Special Appendix. "DE" references district court docket entries.

3. Did the district court properly dismiss a complaint under Rule 12(b)(6) on the basis of 47 U.S.C. 230(c), an affirmative defense, despite that the complaint did not facially establish elements of that defense?

4. Does 47 U.S.C. 230 immunize Facebook from liability for its own tortious conduct, like facilitating terrorist networking and influencing terrorists by controlling information to which they are exposed?

5. Does 47 U.S.C. 230 immunize Facebook for material support of terrorism, independent of any publishing or speaking, simply because Facebook's "speech" might indirectly be implicated?

6. Does 47 U.S.C. 230, enacted to protect minors from objectionable material, protect Facebook's support of terrorism?

7. Assuming 47 U.S.C. 230 otherwise applies, must it yield to the later-enacted and more specific statutes in the ATA, prohibiting material support of terrorism?

8. Assuming 47 U.S.C. 230 otherwise applies, does it void claims under Israeli law, even though choice of law rules bar application of substantive federal law?

## PERTINENT AUTHORITY

The Special Appendix contains pertinent portions of the ATA, 47 U.S.C. 230, and the entire Communications Decency Act (as originally enacted).

## INTRODUCTION

Plaintiffs allege Facebook knowingly provided material resources to, and aided and abetted, Hamas, a designated foreign terrorist organization, violating the ATA. These resources enhanced Hamas' ability to engage in terrorism against plaintiffs, causing death and severe injury. Hamas murdered Taylor Force, Yaakov Naftali Fraenkel, Chaya Zissel Braun, and Richard Lakin and tried to murder plaintiff Menachem Mendel Rivkin. (41-79, 95-112). Plaintiffs are the surviving victim and decedents' estates, and their kin.

Facebook seeks to shirk responsibility, hiding behind 47 U.S.C. 230(c)(1), a provision enacted to protect Internet providers from liability for removing material objectionable for minors. That provision deems content appearing on such websites not attributable to the website. But plaintiffs do not attribute *anything* that Hamas posted on Facebook to Facebook. Instead, they assert Facebook's liability for its own actions and omissions, regardless of the content of Hamas's postings. Providing a designated terrorist organization a platform to distribute anything—whether instructions for upcoming terror attacks or cookie recipes—violates federal civil and criminal law. *See* 18 U.S.C. §§2331(1), 2333(a) & (d), 2339B, 2339C (SPA56 – SPA61); *Holder v. Humanitarian L. Project*, 561 U.S. 1, 31 & 33 (2010). Section 230 is perfectly irrelevant.

## STATEMENT OF THE CASE

### A. Procedural Background

Plaintiffs sue under the ATA and Israeli law for Facebook's knowing provision of high-tech communication and networking services to Hamas and for its subsequent failure to deny those services to Hamas upon being informed of its on-going violations.

After plaintiffs filed their amended complaint ("FAC") (13-136), Facebook moved to dismiss under Rules 12(b)(2) & (b)(6). (137). The district court (Garaufis, *J.*) resolved that motion, simultaneously dismissing two actions against Facebook being litigated in tandem—this one, *Force v. Facebook*, 16-cv-5158, and *Cohen v. Facebook*, 16-cv-4453. (187-214); *Cohen v. Facebook*, 252 F.Supp.3d 140 (E.D.N.Y. 2017). Dismissal of the *Cohen* action was not appealed.

The district court properly established personal jurisdiction over Facebook. (197-203). But it dismissed plaintiffs' claims "without prejudice" under Rule 12(b)(6), holding those claims barred by §230. (203-14) (opinion); (215-16) (judgment).

Plaintiffs timely moved under Rule 59(e) to alter and amend the judgment and separately moved for leave to file a second amended complaint. (217-18). By order entered January 18, 2018, the district court denied both motions. (366-90); *Force v. Facebook*, 304 F.Supp.3d 315 (E.D.N.Y. 2018). Plaintiffs appealed. (433-34).

New evidence arose after plaintiffs noticed their appeal, including congressional testimony of Facebook CEO Mark Zuckerberg, undercover reporting, and empirical research on Facebook's impact on global terror networking. Realizing that much of what Facebook had told the district court was untrue, plaintiffs moved for summary vacatur and remand so the district court could consider the new evidence. On July 17, 2018, a motions panel denied that motion "without prejudice to [plaintiffs] moving in the district court" under Rules 60(b) & 62.1. (Document 90). Plaintiffs filed a still-undecided Rule 60(b) motion on August 6, 2018. (DE 72)

### B. Factual Background

The FAC plausibly alleges, in considerable detail, that Hamas uses and materially benefits from Facebook. (29-41, 117-24). It further plausibly alleges that each of the five terrorist attacks at issue was preceded by considerable dialogue, planning, and networking on Facebook between Hamas terrorists encouraging specific terror attacks at specific locations. Each of the five was likewise followed by Facebook dialogue praising the responsible terrorist and specifically encouraging other terrorists to follow suit. (41-112). The allegations show Facebook's provision of networking and communication services to Hamas proximately caused the terror attacks. *See* (29-124). The FAC also alleges that Facebook had actual knowledge of its support of Hamas and nonetheless persisted materially supporting Hamas. (112-24). It notes in particular that on October 19, 2015, Israeli Prime Minister Benjamin

Netanyahu identified Facebook as the driving force in a wave of murderous attacks, linking Facebook CEO Mark Zuckerberg with Osama Bin Laden. (116-17). Perhaps that was hyperbole, but it certainly got Facebook's attention.

Hamas is terrorist organization. Giving it any material assistance—even in a commercial setting—is illegal. It was first designated by President Clinton in EO 12947 (1995), which, under 50 U.S.C. 1705, makes provision of any funds, goods, or services to, or for the benefit of specially designated terrorists, such as Hamas, a criminal offense. 31 C.F.R. 595.204. In 1997, Hamas was designated a "foreign terrorist organization" under 8 U.S.C. 1189. Providing "material support or resources" to a foreign terrorist organization is a criminal offense. 18 U.S.C. 2339B. "Material support or resources" is defined to include "any property, tangible or intangible, or service, including...expert advice or assistance,...communications equipment, [and] facilities...." 18 U.S.C. §§2339A(b)(1), 2339B(g)(4). The only support excluded by the definition is the provision of "medicine or religious materials." *Id*. "Expert advice or assistance" is defined as any "advice or assistance derived from scientific, technical or other specialized knowledge." §2339A(b)(3).

Facebook has long provided support to Hamas, in constant violation of these provisions. Facebook's primary business is providing a sophisticated social media platform and related products and services. Those services include Facebook's infrastructure, network, networking tools and recommendations, and

communications services. In the overview of its business in its 2013 Annual Report (10-K), Facebook explained the success of its business and advertising rates depends on the "size of [its] user base," the "level of engagement" of its users, and its ability to "add[,] retain[,] and engag[e] active users." Facebook explained that failure to maintain or increase its user base and user engagement negatively impacts its business. (124). Thus, Facebook has strong business incentives to keep user accounts active and to encourage user activity.

Facebook unilaterally gathers information about its users, including every detail that can be gleaned from the user's computer, smartphone, or other internet device. Users may not opt out of most of this data collection; it is imposed as a condition of use. (119). Any information input by a Facebook user and anything else Facebook learns about its users—including the groups they belong to and the people they communicate with—is recorded by Facebook. (118-19).

Facebook mines this data not only to sell targeted advertising, but also to introduce users to other users, groups, events, notices, posts, articles, videos, etc., that its algorithms predict will interest each user. (119-21). It also uses that information to curate the information its users see on their individual Facebook pages, manipulating the content and order of Facebook's "newsfeed" based on predictions of what information Facebook believes likely to get the attention of any particular user. (120). Facebook uses the vast information it gathers about its users

to send each user tailored advertising, news, communications, and networking recommendations. (119-21). People interested in cello get articles about chamber music; people interested in *jihad* get links to Hamas.

These Facebook features are extremely valuable to retailers wanting to attract particular demographics to their product, and likewise to terrorist organizations hoping to attract followers and recruits and to publicize and glorify their actions. Facebook actively connects users with similar interests. (119-21).

Facebook's phenomenal ability to network people with similar interests—including people whose primary interest is terrorism—is well documented. A publicly-available empirical research report released by the Center for Extremism Project ("CEP") in May 2018 documents how Facebook helped form ISIS's global terror network.[1] The report documents its methods and sources and is thus a proper subject for judicial notice. Fed.R.Evid. 201; *see also Apotex Inc. v. Acorda Therapeutics*, 823 F.3d 51, 60 (2d Cir. 2016); *Shaw v. Patton*, 823 F.3d 556, 564 n.12 (10th Cir. 2016).[2] The CEP report has been filed in the district court (DE 72-7)

[1] GREGORY WATERS & ROBERT POSTINGS, SPIDERS OF THE CALIPHATE: MAPPING THE ISLAMIC STATE'S GLOBAL SUPPORT NETWORK ON FACEBOOK (2018), *available at* https://www.counterextremism.com/sites/default/files/Spiders%20of%20the%20Caliphate%20%28May%202018%29.pdf.

[2] At minimum, this Court may certainly use the report as background.

and is the subject of a pending Rule 60(b) motion. (DE 72); *see also* (Document 92) (motion to hold appeal in abeyance pending resolution of Rule 60(b) motion).

The CEP researchers examined 1,000 ISIS accounts on Facebook—a "fraction" of all Facebook ISIS accounts[3]—and tracked them over six months.[4] Some were held by "active IS[IS] fighters" and "prolific [ISIS] propagandists."[5] 730 of the accounts featured posts about ISIS visible to the public. Even so, by the end of the six-month study period, Facebook had removed just 430 of the 1,000 accounts.[6] The CEP study concludes that "Facebook's suggested friends algorithm" linked ISIS "supporters, propagandists, and even fighters" and "aided in connecting extremist profiles and help[ed] expand IS[IS] networks."[7] ISIS uses Facebook to identify new potential terrorists and connect with them, offer them "necessary assistance," and encourage their perpetration of what ISIS calls "'remote control' attacks."[8] Facebook facilitates all that by bringing ISIS supporters together. The CEP study profiles one such example: A male living in Namibia in his late teens or early twenties now has 5,000 Facebook friends, many of whom are ISIS supporters. While he likely made the initial effort to contact ISIS supporters, Facebook drastically

[3] *Id.* at 11.
[4] *Id.* at 7-8.
[5] *Id.* at 11.
[6] *Id.* at 8.
[7] *Id.* at 8.
[8] *Id.* at 11.

improved his access to ISIS terrorists by suggesting such people as new potential "friends."[9] Thanks to Facebook, this Namibian individual now "serves as the most central bridge" between many Indonesian, Filipino, Malagasy, Afghan, and East African ISIS networks.[10] Facebook, the researchers concluded, "facilitate[s]" radicalization and the subsequent connection of new terrorists to ISIS's global terror network.[11] It does so, in part, by "*actively*" bringing terrorists together.[12]

CEP researchers experienced first-hand just how effectively Facebook connects terrorists. They created experimental Facebook profiles. One did not "friend" any terrorists or "like" any posts about ISIS and was used only to view the profiles of ISIS terrorists and supporters. Still, that profile received from Facebook an "influx" of recommended friends who were "IS[IS] supporters, propagandists, and active fighters."[13] Another profile merely "liked" several "non-extremist news pages" about ISIS's capture of Marawi and Facebook inundated it with recommended friends who were Philippine ISIS "supporters and fighters."[14] Another

[9] *Id.* at 24.
[10] *Id.* at 24 & 78.
[11] *Id.* at 77.
[12] *Id.* at 78 (emphasis added).
[13] *Id.* at 78.
[14] *Id.*

profile was used to "friend" just one ISIS account and was then bombarded by Facebook with suggested connections with ISIS terrorists.[15]

Before using Facebook, CEP's researchers did not know the terrorists, did not know or have access to any information about them, and certainly had no means of communicating with them. Facebook changed that, bringing the researchers to these terrorists' digital doorstep. If the researchers had desired to become terrorists themselves, it would have been easy, thanks to Facebook.[16] Indeed, they documented the radicalization of another person on Facebook: An Indonesian ISIS operative found a non-Muslim in New York on Facebook (apparently using Facebook's suggested friends feature) and sent him a "friend" request.[17] Twelve days later, he asked the New Yorker his religion. The New Yorker responded that he had no religion but expressed interest in Islam.[18] Less than *six months* later, the New Yorker had converted to Islam and was affiliated with ISIS. Facebook later introduced him to several active ISIS terrorists operating in the Philippines.[19] As the CEP study notes: "Facebook was the platform that facilitated the [radicalization] process.... [G]iven his connections with existing IS[IS] networks on Facebook, the moment that

---

[15] *Id.*

[16] *Id.*

[17] *Id.* at 76.

[18] *Id.*

[19] *Id.* at 77.

[the New Yorker] wishes to become more than an online supporter[,] he has the necessary contacts available to him."[20]

Facebook has helped introduce thousands of terrorists to one another, facilitating the development of global terror networks. It does so through computer algorithms designed to boost its traffic and thereby its revenue. (119-21, 124). It has thus generated revenue through its support of Hamas. (124). Simultaneously, it provides a great benefit to terrorists, such as Hamas. Facebook's sophisticated platform and services are used by terrorists for networking, communication, logistics, intelligence, public relations, fundraising, and even prestige. Terrorists also use Facebook's services to criminally incite, recruit, and carry out terror attacks around the world, including the attacks at issue in Israel. (29-41).

Facebook has received repeated complaints and warnings that providing services to Hamas and other foreign terrorist organizations violates 18 U.S.C. 2339B. For example, in September 2013, plaintiffs' Israeli counsel wrote Facebook's CEO and General Counsel warning that providing assistance or support to designated terrorists is unlawful. Her letter specifically included Hamas among a list of foreign terrorist organizations. (113). Facebook did nothing.

Facebook is *indifferent* to the destructive impact its services have on terror victims. In a leaked internal memorandum, Facebook's VP of Consumer Hardware,

[20] *Id.*

Andrew Bosworth, opined that Facebook should not shy away from doing things that might cause people to be murdered by terrorists:

> [W]e connect more people. Maybe someone dies in a terrorist attack coordinated on our tools. The ugly truth is that we believe in connecting people so deeply that anything that allows us to connect more people, more often, is de facto good.[21]

Washington Post coverage of this memo noted it remained on "Facebook's internal platform" for nearly two years and was written "almost immediately after a man was shot to death while [live-streaming himself on Facebook], and a few days before a Palestinian teenager was accused of killing an Israeli girl after praising terrorists on Facebook." One former Facebook executive reported that the memo was "super popular internally."[22]

This jibes with Facebook's *modus operandi* in other contexts as well; it acts above the law and with little concern for the social consequences of its business decisions. Largely for that reason, Facebook was recently sued for violating the Fair Housing Act in *Nat'l Fair Housing Alliance v. Facebook* ("*FFHA*"), 18-cv-2689 (S.D.N.Y.) (JGK). There, plaintiffs allege that Facebook gathers, collates, and

---

[21] Avi Selk, *'Maybe someone dies': Facebook VP justified bullying, terrorism as costs of networks' 'growth'*, WASH. POST, March 30, 2018, *available at* https://www.washingtonpost.com/news/the-switch/wp/2018/03/30/maybe-someone-dies-facebook-vp-justified-bullying-terrorism-as-costs-of-growth/?noredirect=on.

[22] *Id.*

evaluates user data to categorize its users across hundreds of demographics, behaviors, and interests, and then encourages advertisers to discriminate by excluding undesirables from their audience. *See NFHA*, 18-cv-2689, Statement of Interest of United States, DE 48 at 4-5 (S.D.N.Y. Aug. 17, 2018). ("*NFHA* Gov't SOI").

### C. The ATA

Congress enacted the ATA in 1992 as a legal complement to existing criminal penalties against terrorists that kill or injure Americans abroad (*see* Pub. L. 99-399, Title XII, 100 Stat. 896 (creating in 1986 what is today Chapter 113B of Title 18)), specifically intending that the civil provisions would not only provide a mechanism for compensating victims of terror, but also serve as an important means of depriving terrorists of financial resources to carry out attacks.[23] It created civil remedies for

[23] State Department Deputy Legal Advisor, Alan Kreczko, testified that the proposed bill "will add to the arsenal of legal tools that can be used against those who commit acts of terrorism against United States citizens abroad." He added:

> We view this bill as a welcome addition to the growing web of law we are weaving against terrorists.... The existence of such a cause of action...may deter terrorist groups from maintaining assets in the United States, from benefiting from investments in the U.S. and from soliciting funds within the U.S.

Statement of Alan Kreczko on S. 2465, Before the Subcommittee on Courts and Administrative Practice (July 25, 1990), https://www.state.gov/documents/organization/28458.pdf. Similarly, a Senate Committee Report explained that the

individuals injured "by reason of an act of international terrorism," defining "international terrorism" to include "acts dangerous to human life that are a violation of the criminal laws of the United States." 18 U.S.C. §§2331(1), 2333(a). It thus made all the criminal prohibitions against terrorism predicate acts to support claims for civil liability, granting victims "threefold the damages he or she sustains and the cost of the suit, including attorney's fees." 18 U.S.C. 2333(a). This Court has held that the phrase "by reason of" demands demonstration of proximate causation (but not but-for causation) as a condition precedent to civil recovery. *Rothstein v. UBS*, 708 F.3d 82, 94-97 (2d Cir. 2013).

Following the 1993 World Trade Center bombing, Congress added 18 U.S.C. 2339A to the list of criminal prohibitions against terrorism, and thus the available predicates for civil liability under the ATA. That statute criminalized providing material support or resources to a terrorist knowing or intending that the support or resources would be used in preparing or conducting terrorist acts. §2339A. Congress again expanded the list in 1996, criminalizing the knowing provision of material support to a foreign terrorist organization. 18 U.S.C. 2339B. Unlike §2339A, §2339B has no scienter requirement, demanding only knowledge of the fact that the recipient is a foreign terrorist organization, not of the organization's intended use of

---

ATA's provision of treble damages "would interrupt, or at least imperil, the flow of money" to terrorist organizations." S.Rep. 102-342 at 22 (1992).

the resources. *Holder*, 561 U.S. at 30-31. In 2002, Congress enacted 18 U.S.C. 2339C, which criminalized the concealment of any material support to a terrorist organization and the provision or collection of funds with knowledge or intent that the funds will be used to cause injury and terrorize a civilian population *or* to violate any one of nine enumerated treaties. §2339C.

In September 2016, Congress enacted the Justice Against Sponsors of Terrorism Act ("JASTA"), Pub. L. 114-222, 130 Stat. 852, amending the ATA and partially abrogating *Rothstein*. 18 U.S.C. 2333, note. JASTA makes liable under the ATA "any person who aids and abets, by knowingly providing substantial assistance, or who conspires with [a] person who committed...an act of international terrorism." 18 U.S.C. 2333(d)(2). Congress found: "International terrorism is a serious and deadly problem that threatens the vital interests of the United States." 18 U.S.C. 2333, note. Congress' stated purpose in passing JASTA was "to provide civil litigants with the ***broadest possible basis***, consistent with the Constitution of the United States, to seek relief against persons...that have provided material support, directly or indirectly, to foreign organizations or persons that engage in terrorist activities...." *Id.* (emphasis added).

### D. The Communications Decency Act[24]

Congress enacted the Communications Decency Act of 1996 ("CDA") as Title V, Subtitle A, of the Telecommunications Act of 1996. Pub. L. 104-104, 110 Stat. 133. (SPA65 – SPA71). As originally enacted, the CDA prohibits certain obscene or harassing communications, §502; modifies the penalty for obscene programing on cable television, §503; requires cable providers to scramble certain cable channels and video programing, §§504-05; authorizes cable operators to refuse certain programing that "contains obscenity, indecency, or nudity," §506; clarifies existing statutory law regarding the communication of obscene materials by computer, §507; criminally prohibits the coercion and enticement of minors to engage in prostitution or "any sexual act," §508; and includes a provision titled "Online Family Empowerment," which does nothing other than create 47 U.S.C. 230, CDA §509. (SPA65 – SPA71). Congress revealed its intent in enacting §230 from its placement within the CDA and its title in its enacting legislation ("Online

[24] The legislative/statutory history provided by some courts, including certain federal appellate courts, about §230 is unfortunately not fully accurate. One relatively minor example appears in this Court's description of §230 as an "amendment" to the CDA. *FTC v. LeadClick Media*, 838 F.3d 158, 173 (2d Cir. 2016). It was not an amendment to the CDA, it was the final provision in the CDA's original enactment. (SPA69).

Plaintiffs cite original legislative documents throughout the following discussion and ask the Court to do the same to hopefully prevent further perpetuation of inaccurate information.

Family Empowerment")—Congress plainly intended §230 to protect the public generally and children specifically from indecent material. *See* §509; (SPA69 – SPA71). Subsection §230(c), which Congress titled "Protection for 'Good Samaritan' Blocking and Screening of Offensive Material" is part of that scheme.

The Senate committee report confirms this. The CDA is intended to

> modernize[] the protections in the 1934 Act against obscene, lewd, indecent, and harassing use of a telephone. These protections are brought into the digital age. The provisions increase the penalties for obscene, harassing, and wrongful utilization of telecommunications facilities; protect privacy; protect families from uninvited cable programming which is unsuitable for children; and give cable operators authority to refuse to transmit programs...which contain obscenity, indecency, or nudity. The measure specifically excludes from liability telecommunications and information service providers and system operators who are not themselves knowing participants in the making or otherwise responsible for the content of the prohibited communications.... The provisions seek to encourage telecommunications and information service providers to deploy new technologies and policies which would allow users to control access to prohibited communications. The incorporation of such technology where reasonable and appropriate would be a defense against liability....

S.Rep. 104-23 at 9, 59 (1995).

The Conference Report likewise describes §230(c) as doing nothing but "protect[ing] from civil liability those providers and users of interactive computer services for actions to *restrict* or to *enable restriction* of access to objectionable online material." H.R.Rep. 104-458 at 194 (1996) (Conf. Rep.) (emphasis added). It

explains that the objective of §230(c) is "to overrule *Stratton-Oakmont* [sic] *v. Prodigy*," for subjecting an Internet provider to liability for restricting access to objectionable material. *Id. Stratton Oakmont* is a New York state court case involving Prodigy's removing some, but not all, the defamatory messages on its site. Analogizing to a newspaper publisher, the court reasoned that Prodigy was responsible for the defamatory messages that remained. *Stratton Oakmont v. Prodigy Services*, 1995 WL 323710, *3-*4 (N.Y. Sup. Ct. May 24, 1995). The Conference Report explains that "such decisions create serious obstacles to the important federal policy of empowering parents to determine the content of communications their children receive through interactive computer services" and thus needed abrogation. H.R.Rep. 104-458 at 194. Clearly, Congress "sought to [protect] the *removal* of user-generated content, not the *creation* of content...." *Fair Hous. Council v. Roommates.com*, 521 F.3d 1157, 1163-64 & n.12 (9th Cir. 2008) (*en banc*) (emphasis in original).

After portions of the CDA were invalidated by *Reno v. ACLU*, 521 U.S. 844 (1997), Congress amended the CDA with the Child Online Protection Act, Title XIV of an omnibus appropriations act. *Ashcroft v. ACLU*, 535 U.S. 564, 569 (2002); Pub. L. 105-277, 112 Stat. 2681-736.[25] Congress made these findings:

[25] Nothing invalidated by *Reno* or expressly upheld by *Ashcroft* is relevant to this litigation.

> (1) while custody, care, and nurture of the child resides first with the parent, the widespread availability of the Internet presents opportunities for minors to access materials through the [Internet] in a manner that can frustrate parental supervision or control;
>
> (2) the protection of the physical and psychological wellbeing of minors by shielding them from materials that are harmful to them is a compelling governmental interest;
>
> (3) to date, while the industry has developed innovative ways to help parents and educators restrict material that is harmful to minors through parental control protections and self-regulation, such efforts have not provided a national solution to the problem....

*Id.* Again, Congress made clear its intent in enacting and later amending the CDA was to protect children from indecent material. Its major contribution was the enactment of 47 U.S.C. 231, which particularly pertains to communications with minors. But it also amended §230, adding subsection (d).

Section 230(b) states the relevant federal policy is to ensure "the continued development of the Internet" and the "competitive free market" in which it operates without significant government regulation while simultaneously "remov[ing] disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material." §230(b)(1), (b)(2), & (b)(4). The references to developing the Internet, the free market, and government regulation appear *nowhere* else in the CDA. (SPA65 – SPA71).

It implements that policy, in part, by declaring "interactive computer services,"[26] such as Facebook, may not "be treated as the publisher or speaker of any information provided by another information content provider." §230(c)(1). "Publisher" and "speaker" are undefined. The statute has no impact on "any...Federal criminal statute," §230(e)(1), but does preempt all inconsistent state and local law. §230(e)(3). It thus creates an affirmative defense to federal civil liability and all liability under state or local law for Internet companies such as Facebook from claims that would treat those companies as the publisher or speaker of certain content provided by someone else. *See* §230(c)(1) & (f)(3).

Section 230 nowhere uses the word "immunity." Plaintiffs are aware of no reference to "immunity" in its legislative history. Many courts nonetheless refer to §230(c) as creating "immunity." That word was first used in explaining §230 by *Zeran v. AOL*, 958 F.Supp. 1124 (E.D. Va. 1997), which used the term without explanation (*e.g.*, *id.* at 1134). The Fourth Circuit followed the district court's lead precisely, thus making "immunity" part of §230 doctrine. *Zeran v. AOL*, 129 F.3d 327, 328 (4th Cir. 1997). The use of that term was unfortunate as it lead to much confusion. The Tenth Circuit recently clarified that §230(c) "provides immunity from liability, not suit," and is thus not similar to more familiar forms of immunity, such as qualified immunity. *Gen. Steel v. Chumley*, 840 F.3d 1178, 1180-82 (10th

[26] "Interactive computer service" is defined by §230(f)(2).

Cir. 2016). It is simply an affirmative defense, no different from any other affirmative defense. *Ricci v. Teamsters Union*, 781 F.3d 25, 28 (2d Cir. 2015) (*per curiam*); *Doe v. GTE Corp.*, 347 F.3d 655, 657 (7th Cir. 2003); *see also Zeran*, 129 F.3d at 329-30 (calling §230 an "affirmative defense").

To prevail on this affirmative defense, a defendant must show 1) it provides an "interactive computer service," 2) a claim based on information provided exclusively by "another information content provider" that 3) "would treat the defendant as the publisher or speaker of that information." *LeadClick*, 838 F.3d at 173; §230(c)(1) & (f)(3). An "information content provider" is "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." §230(f)(3). Thus, §230 expressly withdraws its defense from any defendant that either created or developed (both terms undefined) any part of the offending content. *Id.*; *Roommates.com*, 521 F.3d at 1163; *Ricci*, 781 F.3d at 27-28; *NFHA* Gov't SOI at 13-14.

### E. Procedural History

Plaintiffs assert claims under the ATA for aiding and abetting, conspiracy, provision of material support to terrorists, and provision of material support to a terrorist organization (125-29) and claims under Israeli law for negligence, "breach of statutory duty" (a recognized Israeli tort), and for aiding and abetting under Israeli

law. (129-35). Facebook moved to dismiss under Rule 12(b)(2) & (b)(6), arguing lack of personal jurisdiction, "immunity" from liability under §230, and failure to state an ATA claim. *See* (137). Following oral argument (138-185), the district court dismissed the complaint on May 18, 2017. (187-216).

The district court first made specific findings about Facebook's services, stating particularly that "Facebook *generates* targeted recommendations" for its users and "*promot*[*es*] content, websites, advertisements, [other] users, groups and events that may appeal to a [particular] user based on their usage history." (189) (emphasis added). "In this way," continued the district court, "Facebook *connects* users with other individuals and groups based on *projected* common interests, activities, contacts, and patterns of usage." (189) (emphasis added). "Facebook also *presents* [particular] users with [particular] content...that is likely to be of interest to [those users], again based on prior usage history." (189) (emphasis added).

It correctly held that Facebook is subject to personal jurisdiction in New York for suits under the ATA (199-201) and properly asserted supplemental jurisdiction over the Israeli law claims. (202-03).

Relying on §230, the district court dismissed all claims. (203-13).[27] *First*, it held Facebook is an interactive computer service. (205). *Second*, relying on footnoted *dicta* from a district court in a different circuit, it held none of the content at issue was created or developed by Facebook, which would have precluded §230 immunity. (205) (citing *Klayman v. Zuckerberg*, 910 F.Supp.2d 314, 321 n.3 (D.D.C. 2012)).[28] *Third*, the court held that all of plaintiffs' claims necessarily treat Facebook "as the publisher or speaker" of Hamas's content, even though publishing or speaking is neither an element of the ATA nor independently sufficient for ATA liability. (205). The district court argued the decision whether to permit a post to remain on Facebook or to remove it falls within "the editorial prerogative" and thus plaintiffs' claims seek to assert liability related to Facebook's publishing duties. (206-07). *Fourth*, the court held §230 applies, despite the strong presumption against extraterritorial application of statutes, because the statute's "focus" is simply "limitation on liability" and thus applies in any court where that limitation is enforced. (211-12).

---

[27] The court imprecisely referenced "Section 230[] of the Communications Decency Act." (203). The statute is actually either Section 509 of the CDA or Section 230 of Title 47. (SPA69).

[28] *See* 47 U.S.C. 230(f)(3) (defining an "information content provider" as one "responsible, in whole or in part, for the *creation or development* of information" (emphasis added)).

The district court specifically dismissed "[t]he Amended Complaint" without prejudice. (214). Judgment issued the same day, likewise stating the FAC was dismissed "without prejudice." (215-16).

On June 15, 2017, plaintiffs moved under Rule 59(e) to alter or amend the judgment (217) and simultaneously moved for leave to amend the complaint. (218). Their proposed Second Amended Complaint ("SAC") is in the Appendix (227-365). Its principal differences with the FAC are summarized. (223-26). The SAC further details the services Facebook provided Hamas, including its provision of "personnel" and "expert assistance," as those terms are used in the ATA. (223-24, 249-54). It explains that Facebook's obligations to refrain from providing services to Hamas derives from the terrorists' identities, not the content of their speech, and alleges that Facebook had the ability to restrict access to Facebook based on identity. (224, 252-53). It also alleges that Facebook's content review of the Hamas postings took place in Ireland and Israel, not in the United States. (225, 348-49).

Finally, the SAC expands the claim for aiding and abetting liability, alleging many predicate acts by Hamas plainly not dependent upon attributing Hamas' content to Facebook (225, 353-54), and adds a new claim, under 18 U.S.C. 2339C, alleging that Facebook concealed its provision of material resources to Hamas. (225, 257, 340-41, 357-58).

The district court denied both motions in January 2018, reiterating its prior holdings and unfairly criticizing plaintiffs for failing to have previously raised counter-arguments to Facebook's purported affirmative defense under §230. This criticism was unfair considering that plaintiffs' earlier substantive filing was an opposition to a motion to dismiss, which merely responded to the motion to dismiss. Facebook had not filed an answer asserting any affirmative defenses. (408-32). As for the new claim for concealment, the district court held that §230 provides no defense, but plaintiffs failed to plead plausibly that Facebook "concealed or disguised" Hamas' use of Facebook's platform. (430-31).

This timely appeal followed. (433-34).

## SUMMARY OF ARGUMENT

Plaintiffs sue Facebook under the ATA for supporting, aiding and abetting, and conspiring with Hamas. Facebook asserts immunity under a provision of the CDA, a statute intended to protect children from offensive content on the Internet, which was never intended to confer immunity for supporting terrorism.

The CDA cannot be applied extraterritorially to ATA claims arising overseas that have no U.S. contacts. Nor does it trump the later-enacted ATA or Israeli law for claims arising in Israel. It certainly does not apply here given that Facebook's duties arise not as a publisher of Hamas's substantive communications and given

that Facebook encouraged those communications and uses them to create services for Hamas.

Even if CDA immunity were a valid defense, Facebook asserts it prematurely. As an affirmative defense, it must be presented in Facebook's yet-to-be filed answer.

## STANDARD OF REVIEW

This Court "review[s] *de novo* the grant of a motion to dismiss, accepting all factual allegations in the complaint as true and drawing inferences from those allegations in the light most favorable to the plaintiff." *McDonough v. Smith*, __ F.3d __, 2018 WL 3672942 at *3 (2d Cir. Aug. 3, 2018). It generally reviews denial of leave to file an amended complaint for abuse of discretion, unless (as here) the denial was for futility, "in which case [the] review is *de novo*." *Allen v. Credit Suisse*, 895 F.3d 214, 227 (2d Cir. 2018). Further, since the FAC was dismissed "without prejudice," nothing prohibited plaintiffs from filing a new complaint; they did not need leave to amend. *See* Wright & Miller, Fed. Prac. & Proc. Civ. §1505 (3d ed.). Their SAC therefore should have been accepted as filed and then separately dismissed under Rule 12(b)(6) if the court below found it insufficient. Failing to do so was legal error. Dismissal of the SAC should accordingly be reviewed *de novo*.

## ARGUMENT

### I. Section 230 Does not Apply Extraterritorially

"[L]egislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States" because Congress "is primarily concerned with domestic conditions." *Morrison v. Nat'l Australia Bank*, 561 U.S. 247, 255 (2010). "When a statute gives no clear indication of an extraterritorial application, it has none." *Id.* *Morrison* lamented that, for decades, many courts had "disregard[ed] the presumption against extraterritoriality" and hoped finally to end that practice. *Id.* at 255, 261.

*Morrison* itself recognized that the presumption against extraterritoriality is not usually self-executing because "it is a rare case of prohibited extraterritorial application that lacks *all* contact with the territory of the United States." *Id.* at 266 (emphasis in original). But the presumption "would be a craven watchdog indeed if it retreated to its kennel whenever *some* domestic activity is involved." *Id.* (emphasis in original). Instead, only certain especially significant domestic contacts count in the extraterritoriality analysis. *Id.*

The district court erroneously dismissed this case based on §230(c)(1) although *all* acts occurred overseas and §230 gives no clear indication of extraterritorial application. (210-11). Indeed, this is the "rare" easy case that lacks *all* contact with United States territory. It is being litigated here because the ATA, which explicitly applies extraterritorially, grants victims of international terrorism

who are U.S. nationals access to U.S. courts, 18 U.S.C. 2333(a), allowing litigation over acts that "occur primarily outside the territorial jurisdiction of the United States." 18 U.S.C. 2331(1).

Apparently eager to reach §230,[29] the district court cited the Supreme Court for the assertion that "all questions of extraterritoriality should be assessed using a two-step framework." (209) (internal quotation marks omitted). But the Supreme Court never demanded a two-step process. Instead, it stated that in two close cases (*Morrison* and *Kiobel*, *infra*), the Court had in fact used "a two-step framework for analyzing extraterritoriality issues." *RJR Nabisco v. European Community*, 136 S.Ct. 2090, 2101 (2016). Far from questioning *Morrison's* statement that absent relevant domestic contact, application of the presumption against extraterritoriality is easy, *RJR Nabisco* reaffirmed it: "When a statute gives no clear indication of an extraterritorial application, it has none." *Id.* at 2100. It expressly noted that in an earlier case the Court needed not proceed to the second step. Finding that "all the relevant conduct...took place outside the United States," the Court's work was done. *Id.* at 2100-01 (quoting *Kiobel v. Royal Dutch Petroleum*, 569 U.S. 108, 124 (2013));

[29] The district court may have been confused over what plaintiffs' claims mean and what its duties were. In a different context, the district court asserted: "[T]he task before the court is not to interpret the ATA, but to determine the meaning of Section 230(e)(1)." (423). Yet plaintiffs' claims arise under the ATA, not §230, which, at worst, is merely a defense against those claims. The district court put the cart before the horse.

*see also Licci v. Lebanese Canadian Bank*, 834 F.3d 201, 214-15 (2d Cir. 2016) (with no relevant U.S. contact, "the inquiry, in all likelihood, ends").

Plaintiffs were injured overseas by terrorists who operated overseas and interacted overseas. (29-112). The material support the terrorists received from Facebook derived from Facebook employees or agents in Ireland and Israel, not the U.S. (348-49). No domestic contacts warrant more inquiry. This is the easy case *Morrison* imagined: §230 provides no defense to claims arising entirely overseas.

The district court mistakenly approached the question differently. It presumed a requirement to conduct a two-step inquiry and jumped into the second step without having identified a single important domestic contact. (210-13). It applied the second step incorrectly as well, as plaintiffs explain shortly.

The purpose of the second step—to be used only in far closer cases—is to "determine whether the case involves a domestic application of the statute" by "looking to the statute's 'focus.' If the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad[.]" *RJR Nabisco*, 136 S.Ct. at 2101. A statute's "focus" is "the object of its solicitude, which can include the *conduct* it seeks to regulate, as well as the *parties* and *interests* it seeks to protect or vindicate." *WesternGeco v. ION Geophysical*, 138 S.Ct. 2129, 2137 (2018) (cleaned up) (emphasis added). A "focus" may not be derived in a vacuum. "If the statutory

provision at issue works in tandem with other provisions, it must be assessed in concert with those other provisions." *Id.* Significantly, courts must identify the focus of the *entire* enactment, not a single statute. *Morrison*, 561 U.S. at 266-68 (referencing "the focus of the Exchange Act" as a whole); *Matter of Warrant to Search a Certain E-Mail Account*, 829 F.3d 197, 217-20 (2d Cir. 2016), *vacated on other grounds*, 138 S.Ct. 1186 (2018). When determining statutory focus, "it is helpful to resort to the familiar tools of statutory interpretation, considering the text and plain meaning of the statute, as well as its framework, procedural aspects, and legislative history." *Id.* at 217 (internal citation omitted).

The entirety of the CDA (SPA65 – SPA71) and its legislative history (*supra*) make clear that the focus of the CDA (not merely §230) is regulation of indecent and objectionable material on the Internet. Section 230(c) in particular was written to protect responsible Internet companies removing objectionable content from their websites and to facilitate development of blocking and filtering technology. S.Rep. 104-23 at 59; H.R.Rep. 104-458 at 194; *see also Roommates.com*, 521 F.3d at 1163-64 & n.12. That is implied from the statutory text itself, which does not mention "immunity" but, in some cases, forbids courts from "treat[ing]" certain Internet companies as a "publisher or speaker" of content on its website. §230(c)(1). It appears under the title "Protection for 'Good Samaritan' Blocking and Screening of Offensive Material"; as the Seventh and Ninth Circuits have held, §230 should be

interpreted consistently with that caption. *Roommates.com*, 521 F.3d at 1164. Its purpose, as a part of the CDA, is to prevent objectionable material from being attributed to the website where it appears, making it safer for Internet companies to self-regulate content. H.R.Rep. 104-458 at 194 (Conf. Rep.); *Roommates.com*, 521 F.3d at 1163-64 & n.12.

Thus, the only contacts germane to extraterritoriality analysis are contacts relevant to the objectionable material appearing on Facebook. Here, all such contacts are in Israel, the West Bank, Gaza, and, if Facebook manually reviewed the postings, possibly the location where that review occurred (likely Ireland). These are the locations where the offensive content was posted to Facebook, where the intended recipients were located, where Facebook's services forged relationships and enabled communication among terrorists, where complaints about the posts were made to Facebook, and where Facebook possibly reviewed the offensive content. Nothing occurred in the United States.

The district court, however, held that §230's focus is "its limitation on liability." (211). This statement suffers many problems:

1. A statute's "focus" is not determined by the single sentence of interest in a given case. *WesternGeco*, 138 S.Ct. at 2137. The 26 words of §230(c)(1) limit liability (to facilitate removal of offensive content). The 4,478 words of the Communications *Decency* Act protect children from objectionable material. The

focus of 4,478 words cannot be determined by looking only at 26 cherry-picked words.

2. Limiting liability is neither conduct, nor party, nor interest that Congress desires to protect or vindicate. *See id.* It cannot fairly be described as the "focus" of a statute.

3. The relief provided by a statute "is not necessarily its focus." *Id.* at 2138. Relief is simply "the means by which the statute achieves its end." *Id.* Section 230(c)(1) indeed limits liability. But that is just how the statute "remove[s] disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material" with minimal government interference. §230(b). By calling §230's limitation on liability the CDA's "focus," the district court conflated focus and effect.

4. Declaring that the *focus* of the CDA is limiting liability oversimplifies matters. If Facebook used its website to steal users' bank information, its liability certainly would not be limited by the CDA. So too for using its website to materially support terrorism. Painting in broad strokes, the district court managed to obscure the subject it was analyzing.

5. If Congress had desired simply to limit liability of Internet companies, it would have made them "immune from liability" arising out of content first authored by another person. Section 230 is intended to do something different.

6. "Given that [§230(c)(1)] limits [its reach] to suits [involving acts that would constitute publishing or speaking], the suits must be based on [such conduct (*i.e.*, publishing or speaking)] occurring in the territory of the United States." *See Loginovskaya v. Batratchenko*, 764 F.3d 266, 272 (2d Cir. 2014).

7. By the district court's rationale, every statute that in some way constrains a cause of action to particular facts (such as creating an element of a claim), shortens a statute of limitations, or limits jurisdiction, would likewise have the focus of limiting liability. A statutory focus cannot be simply to limit (or expand) liability. Indeed, even a tort reform statute—reflecting a policy of limiting liability—would not have the "focus" of liability limitation. The focus of such a statute would be regulating compensation to victims of tortious injury. The extraterritoriality analysis would look not to the location of the court but to the location of the tortious conduct or the plaintiff's injuries.

Upon wrongly concluding that the CDA's focus is limiting liability, the district court found Facebook's invocation of §230 was domestic because the court assesses liability and it sits in the United States, not Israel, Gaza, Ireland, or anywhere else. (212-13). That holding erroneously renders the CDA, and every other

liability-limiting statute, exempt from the presumption against extraterritoriality. The Supreme Court has issued four opinions since 2010 (*Kiobel*, *Morrison*, *RJR Nabisco*, and *WesternGeco*) aimed at getting lower courts to take the presumption against extraterritoriality seriously.

## II. Rule 12(b)(6) Dismissal for an Affirmative Defense is Inappropriate Since the Complaint Does Not Make the Defense Inevitable

Section 230(c)(1) provides an affirmative defense no different from any other affirmative defense. *GTE Corp.*, 347 F.3d at 657; *Gen. Steel*, 840 F.3d at 1180-82; *Ricci*, 781 F.3d at 28. Accordingly, a defendant must raise it in an answer, Rules 8(c) & 12(b), and must plead the elements of the defense. *Bethpage Water v. Northrop Grumman*, 884 F.3d 118, 125 (2d Cir. 2018).

Facebook has not filed an answer. It asserted §230 "immunity" in its motion to dismiss. Courts may dismiss an action under Rule 12(b) based on an affirmative defense not listed in Rule 12(b) only when "the statute's barrier to suit is evident from the face of the complaint." *Ricci*, 781 F.3d at 28. Facebook nowhere argued its entitlement to dismissal is facially evident from the complaint. The district court thus twice erred, first shifting Facebook's burden to prove *its* affirmative defense onto plaintiffs, and second finding that affirmative defense applicable despite the complaint not facially supporting that finding.

"Affirmative defenses do not justify dismissal under Rule 12(b)(6); litigants need not try to plead around defenses." *GTE Corp.*, 347 F.3d at 657. Plaintiffs had no obligation to try to plead around §230. They alleged facts adequate to support their claim under the ATA and foreign law. The face of the complaint does not plainly implicate §230. Thus, dismissal based on §230 was improper.

This Court's decision in *Ricci* and the D.C. Circuit's decision in *Klayman v. Zuckerberg*, affirming Rule 12 dismissals under §230, provide the district court no support. *Ricci* was an action for defamation. *Ricci*, 781 F.3d at 27. The complaint stated claims against a computer service, treating it as a publisher or speaker of information written by others. *Id.* The *Ricci* plaintiffs thus pleaded the elements of §230(c) on the face of the complaint. *Id.* at 28. *Klayman* involves claims for assault and negligence against Facebook for its failure to remove threatening or dangerous Facebook posts. *Klayman v. Zuckerberg*, 753 F.3d 1354, 1356-57 (D.C. Cir. 2014). The *Klayman* plaintiff asserted Facebook had assaulted him and acted negligently toward him by breaching the duty of care that Facebook allegedly owed him. *Id.* The D.C. Circuit held the complaint facially pleaded a §230 defense; it alleged that Facebook and Zuckerberg were both providers of an "interactive computer service" and that both were allegedly liable as the "publisher" of content produced by another. *Id.* at 1357-59.

Plaintiffs' complaint here most certainly does not facially plead that Facebook did not develop offending content. Rather, it plausibly alleges, as plaintiffs explain *infra*, that Facebook *is* a developer (at least "in part" (§230(f)(3))) of the offending content. Similarly, the complaint pleads that speaking and publication have *nothing* to do with their ATA claims and that the acts complained of are not the acts of a traditional publisher (*see infra*).

Facebook believes it can nonetheless prove entitlement to the §230 defense. It may try, but only after the parties have had discovery and the case progresses to summary judgment or trial. Given what has been revealed since the district court issued its initial opinion, such as the CEP study (*supra*), it appears likely discovery will reveal Facebook as a developer of significant offending content sufficient to support plaintiffs' ATA claims. The district court's resolution of the §230 affirmative defense so early wrongly put the defense before the claim.

## III. Plaintiffs' ATA Claims are Properly Stated

All one must do to violate 18 U.S.C. 2339B is "knowingly provide[] material support or resources to a foreign terrorist organization," knowing that the organization is a foreign terrorist organization, but not necessarily desiring to further its terror activities. §2339B; *Holder*, 561 U.S. at 30-31, 33. "Material support" is defined so broadly as to include nearly anything, "tangible or intangible," except for "medicine [and] religious materials." 18 U.S.C. §§2339A(b)(1), 2339B(g)(4).

"Material support" includes even the provision of "technical or specialized knowledge." §2339A(b)(3).

The FAC alleges Facebook provided valuable services to Hamas, providing many specific examples, that doubtlessly meet the broad statutory definition of "material support." (29-41, 112-21). It further plausibly alleges these material support and resources were used to prepare or carry out acts of terrorism. (37-41); *see also* (41-112). The FAC alleges facts from which it may reasonably be inferred that Facebook knew or was willfully blind to Hamas's designation as a foreign terrorist organization and that Facebook knew Hamas had engaged and engages in terrorist activity as defined by §2339B. (25-29, 112-13, 128-29). Plaintiffs thus state a valid claim under §2339B.

Section 2339A differs from §2339B mainly in that the former applies to the material support of individual terrorists, rather than an organization, and requires that the material supporter "know[] or intend[]" that the material support (defined just as in §2339B) be "used in preparation for, or in carrying out" acts of terrorism. §2339A. This standard is met as well. The FAC alleges many facts from which it may reasonably be inferred that Facebook knew or was willfully blind to its users being Hamas operatives and using Facebook to facilitate terrorism. (25-29, 41-113, 128-29). Plaintiffs specifically alleged that Facebook refused to actively monitor its network to block Hamas's use of Facebook; even when receiving specific

complaints about Hamas terrorists using Facebook, Facebook either did nothing or deleted only some of the content on the terrorists' Facebook pages, allowing the terrorists to continue using Facebook. (114-16, 121-24). Plaintiffs also alleged Hamas, its leaders, and affiliates, maintain Facebook accounts in their own names openly displaying emblems and symbols of Hamas. (33-36). Facebook, through its subsidiary Facebook Payments, Inc., is a registered money services business (*see* https://www.fincen.gov/msb-registrant-search), and as such needs to monitor its money service customers to comply with counter-terrorism regulations using the U.S. Treasury's publicly available list of specially designated terrorists and terrorist organizations and their aliases. Facebook could easily have used the same list to ensure it does not provide Facebook accounts to designated terrorists including Hamas. (113). That filtering would have been entirely electronic and easy to administer.

By properly articulating liability under §§2339A, 2339B, a plaintiff states valid claims against the material supporter under §2333(a), provided that he alleges "acts dangerous to human life" that "appear to be intended" to coerce or influence government or the civilian population. §2331(1); *see Boim v. Quranic Literacy Inst. & Holy Land Found.*, 291 F.3d 1000, 1015 (7th Cir. 2002) ("If…[defendants] violated…2339A or section 2339B, that…would…be sufficient to meet the definition of 'international terrorism' under…2333 and 2331."); *Goldberg v. UBS*,

660 F.Supp.2d 410, 426-27 (E.D.N.Y. 2009). Plaintiffs meet that standard. (30-32, 39); *Boim v. Holy Land Found.*, 549 F.3d 685, 690 (7th Cir. 2008) (*en banc*) ("Giving [resources] to Hamas, like giving a loaded gun to a child (which also is not a violent act), is an 'act dangerous to human life.'").

A plaintiff asserting a claim against a primary actor under the ATA must plead proximate causation. *Rothstein*, 708 F.3d at 94-97. As the term is "ordinarily used," a plaintiff need allege only that the defendant's actions were "'a substantial factor in the sequence of responsible causation,' and that the injury was 'reasonably foreseeable or anticipated as a natural consequence.'" *Strauss v. Crédit Lyonnais*, 925 F.Supp.2d 414, 432 (E.D.N.Y. 2013) (quoting *Lerner v. Fleet Bank*, 318 F.3d 113, 123 (2d Cir. 2003)). Thus, "plaintiffs who bring an ATA action are not required to trace specific dollars to specific attacks.... Such a task would [typically] be impossible and would make the ATA practically dead letter...." *Id.* at 433. It is enough to support the inference that Facebook's material support of Hamas "was a substantial reason that Hamas was able to perpetrate the terrorist attacks at issue, and that Hamas' increased ability to carry out deadly attacks was a foreseeable consequence" of Facebook's material support. *Id.* at 432; *Rothstein*, 708 F.3d at 91-92 (quoting *Lerner*, *supra*).

ATA plaintiffs need not establish but-for causation. *Boim*, 549 F.3d at 690, 695-97; *Linde v. Arab Bank*, 97 F. Supp. 3d 287, 323-29 (E.D.N.Y. 2015), *vacated*

*on other grounds*, 882 F.3d 314 (2d Cir. 2018). Congress enacted the ATA to impede terrorism by imposing liability "at any point along the causal chain of" support. *Id.* at 326. Requiring terror victims to establish but-for causation would impose a virtually insurmountable bar, "eviscerate[ing] the civil liability provisions of the ATA." *Id.*

The FAC alleges detailed facts showing Hamas's use of Facebook's services since at least 2011 to carry out essential functions of the organization and its terrorist activities. These resources strengthen Hamas internally as an organization (*e.g.*, providing communication, logistics, and networking capabilities, and freeing funds for other terrorist activities), as well as externally (*e.g.*, enabling Hamas to build local public support, generate a cult of hatred and violence, and recruit more followers). Plaintiffs provided specific examples of Hamas using Facebook before, during, and after each attack at issue to bolster their terrorist operations and make such attacks more likely and more effective. (41-112). Plaintiffs have thus sufficiently alleged proximate causation.

With the enactment of JASTA, the ATA now explicitly authorizes substantive causes of action for aiding and abetting and conspiracy liability. §2333(d). As for causation, plaintiffs pleading secondary liability need only allege that "the Hamas terrorists who committed the...attacks at issue caused plaintiffs' injuries, whether as

a matter of proximate or but-for causation." *Linde v. Arab Bank*, 882 F.3d 314, 331 (2d Cir. 2018). Plaintiffs easily meet that standard. (41-112).

Congress directed courts to follow *Halberstam v. Welch*, 705 F.2d 472 (D.C. Cir. 1983), in assessing secondary liability under the ATA. *Id.* at 329; §2333, note. To state an aiding and abetting claim under the ATA, plaintiffs must allege:

> (1) the party whom the defendant aids must perform a wrongful act that causes an injury; (2) the defendant must be generally aware of his role as part of an overall illegal or tortious activity at the time that he provides the assistance; [and] (3) the defendant must knowingly and substantially assist the principal violation.

*Halberstam*, 705 F.2d at 477. All three elements are satisfied here. The FAC certainly alleges injury due to Hamas's illegal terrorist activities. It also alleges and supports the plausible inference that Facebook was "generally aware" of its role in Hamas's terrorist activities. The FAC contains many allegations and examples of Hamas, its leaders, and affiliates openly maintaining and using Facebook accounts in their own names and with the emblems and symbols of Hamas. (33-36). It also plausibly alleges Facebook has failed to exclude terrorists from its system even when having actual knowledge of their presence. (114-16, 121-24). Finally, plaintiffs plausibly allege Facebook knowingly and substantially assisted Hamas' terrorism.

To state a conspiracy claim under the ATA, plaintiffs must allege "an agreement to do an unlawful act or a lawful act in an unlawful manner; an overt act in furtherance of the agreement by someone participating in it; and injury caused by

the act." *Halberstam*, 705 F.2d at 487. All three elements are satisfied. The FAC alleges that "Facebook conspired with Hamas" (127), offering examples in which Facebook knowingly permitted Hamas terrorists to operate on Facebook, sometimes after half-heartedly shutting down an account after being pressured to do so. *E.g.* (115-17, 121-24). The "overt act" is simply Facebook permitting or re-establishing Hamas accounts after briefly shutting them down. Finally, plaintiffs have alleged injuries resulting from Facebook's knowing support of Hamas terrorists.

## IV. Section 230(c)(1), Even if Applicable, Provides No Defense

Facebook asserted below that in *Ricci*, a dissimilar case not involving Facebook, this Court "joined a growing number of [courts] recognizing that Facebook in particular is immune from claims analogous to those raised here." (DE 35 at 9). It cited seven cases involving Facebook, asserting that they are all consistent with a "national 'consensus'" that §230 immunizes Facebook. *Id.* at 9-10.

Just this week, the Department of Justice criticized Facebook for similar language: "Facebook paints with too broad a brush in asserting that 'courts repeatedly have held that the CDA protects Facebook from claims arising from it[s] publication of content created by third parties[.]'" *NFHA* Gov't SOI at 16. As the DOJ notes, each case must be viewed in context. *Id.* In the present context, the Court need not even reach the CDA for reasons explained *supra*. If it does, it will have three independent reasons for finding that §230 provides Facebook no defense.

The "Internet has outgrown its swaddling clothes and no longer needs to be...gently coddled." *Roommates.com*, 521 F.3d at 1175 n.39. It "has become...the preeminent...means through which commerce [and much else] is conducted.... [I]ts vast reach into the lives of millions is exactly why we must be careful not to exceed the scope of the immunity provided by Congress...." *Id.* at 1164 n.15. Congress created a narrow immunity necessary to facilitate the removal of offensive content and the development of blocking and filtering technology. It must not be expanded to do anything further, lest it "create a lawless no-man's-land on the Internet." *Id.* at 1164.

### A. Section 230(c)(1) Was Not Intended to and Does Not Shield Facebook for its Own Content Development

Only a defendant that "*passively* displays content…created *entirely* by third parties" is immune under §230(c) as an "interactive computer service" provider. *Id.* at 1162 (emphasis added). A defendant that assists or "participate[s]," even "in part," in the "development" of "what made the [offending] content unlawful," is an "information content provider" and is not protected by §230(c). §230(f)(3); *LeadClick*, 838 F.3d at 174-76; *Roommates.com*, 521 F.3d at 1162-63. Although "development" is undefined by statute, case law establishes that little is needed to find an Internet company republishing someone else's content a developer-in-part: Simply requiring users to provide specific information as a condition on use is

sufficient (by compelling users to supply information, the defendant is "much more than a passive transmitter of information"). *Id.* at 1166. So too unlawfully selectively directing certain content to certain selected users or unlawfully "steer[ing] users" to particular information or people. *Id.* at 1167. When an Internet provider aggressively uses information as part of its business or "encourage[s] illegal content," it ceases to be a passive re-publisher and becomes an active participant in the development of that information. *Id.* at 1172, 1175. Even merely "encourag[ing]" third parties to post unlawfully defeats §230 immunity. *Id.* at 1171; *Huon v. Denton*, 841 F.3d 733, 742 (7th Cir. 2016) (encouraging the "most defamation-prone commenters" to write comments forfeits CDA immunity). All that is needed to be a developer is to augment the content in some way and to contribute to its alleged unlawfulness or to "specifically encourage[] development of what is offensive about the content." *Roommates.com*, 521 F.3d at 1168; *LeadClick*, 838 F.3d at 174-76 (quoting *Roommates.com*); *FTC v. Accusearch*, 570 F.3d 1187, 1199 (10th Cir. 2009).

The word "develop" "derives from the Old French *desveloper*," which means to make something "visible, active, or usable." *Id.* at 1198 (internal quotation marks omitted). Thus, when a photograph is transformed from a blank sheet of photo paper with a latent image into a photograph, it is "developed." *Id.* When "untapped potential for building or for extracting resources" is realized on land, that land is "developed." *Id.* Development does not connote creation of something new. It

merely requires improving something to render it more available or usable. Thus, when third-party content is analyzed by Facebook to suggest new relationships, networking opportunities, stories of interest, etc., Facebook "develops" the third-party content.

To avoid "developer" status, an Internet provider must remain vigilantly "'neutral' with respect to generating offensive content." *Accusearch*, 570 F.3d at 1201. As Senator Cruz put it during Mark Zuckerberg's congressional testimony, it must be a public forum and steadfastly avoid becoming a "First Amendment speaker." (DE 72 at 7) (Rule 60 motion quoting public testimony).[30]

Facebook's *modus operandi* is to actively and purposefully develop content. Facebook makes its money by getting its users hooked. Extreme and offensive content is Facebook's "crack cocaine." (DE 72 at 11) (Rule 60 motion quoting publicly aired documentary).[31] One of Zuckerberg's former mentors explains that offensive content is exceptionally valuable to Facebook because it galvanizes others, increasing their use of Facebook and thus Facebook's revenue. *Id.* Facebook permits much content that violates its rules to remain on its website. As a Facebook content

---

[30] *Available at* Transcript of Mark Zuckerberg's Senate hearing, Wash. Post, Apr. 10, 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?noredirect=on&utm_term=.a90bc769a600.

[31] *Available at* Channel 4, *Inside Facebook: Secrets of the Social Network*, https://www.youtube.com/watch?v=8Qc3wpS6IVc.

monitor explained, not realizing he was being filmed by an undercover reporter, "[i]t's all about making money at the end of the day." *Id.*

Facebook develops the posts of its users in two fundamental ways:

### *1. Facebook Facilitates Terror Networking and Communication*

As explained *supra*, Facebook brings terrorists and would-be terrorists together. It analyzes the content of user posts and the way users use Facebook. It compels users to divulge information about themselves as a condition of use. Based on all Facebook learns about the user, it automatically suggests potential new "friends," selectively bringing specific people together. When the user is a terrorist, Facebook suggests other terrorists as friends. It thus managed to transform a Namibian lone wolf into "the most central bridge" between far-flung terror networks. (*Supra*). It identifies potential terrorists by analyzing their interests—such as by analyzing the news stories they read—and puts them in contact with active terrorists so they may be further radicalized. (*Supra*). For its own profit, Facebook actively, purposefully, and intentionally brings terrorists together who would have no other means of finding one another.

Facebook thus constantly violates many federal criminal statutes intended to counter terrorism. *E.g.* 18 U.S.C. 2339A, 2339B, 2339C (*see supra*). It is thus civilly liable under the ATA. By actively developing such content, it forfeits immunity under the CDA. *Accord NFHA* Gov't SOI at 17-21.

### *2. Facebook Encourages Terrorists to Communicate and Selectively Organizes, Prioritizes, and Limits Access to User Content to Influence and Control Other Users*

A defendant may be liable for seemingly re-publishing content of another party if its presentation or organization of that material is designed or intended to influence the intended recipient's response to that information. *Roommates.com*, 521 F.3d at 1165, 1171; *Doe v. Internet Brands*, 824 F.3d 846, 852-53 (9th Cir. 2016) ("CDA does not declare 'a general immunity from liability deriving from third-party content.'") ("Congress has not provided an all[-]purpose get-out-of-jail-free card...."). Indeed, action that merely "increase[es] the likelihood that" the intended audience of the information might react in a desired manner renders the defendant an "information content provider," and thus not immune under §230. *LeadClick*, 838 F.3d at 176.

Facebook does more than facilitate networking. It controls what people see and how they think by selecting posts, friends, and information that its users see based on what Facebook believes will cause the user to use Facebook as much as possible. Indeed, Facebook has admitted to manipulating the "newsfeed" of 689,000 users to *control their feelings*![32] Facebook admits it "ha[s] discovered how to make

[32] *Facebook Reveals News Feed Experiment to Control Emotions*, The Guardian, June 29, 2014, https://www.theguardian.com/technology/2014/jun/29/facebook-users-emotions-news-feeds.

users feel happier or sadder" by controlling exposure to emotional content.[33] It uses the same know-how to radicalize by causing people with a passing interest in terrorism to be exposed to terror-related content and by "feeding" them stories and data likely to engage them.

Facebook provides Hamas with services it likely could not find elsewhere. Facebook facilitates Hamas's communication with its own members and potential recruits, helps with logistics and planning by bringing Hamas information that otherwise would have been difficult to uncover, handles Hamas' public relations by distributing its messages much farther and with far more precision than any press release possibly could, and assists with fundraising by bringing Hamas into communication with potential donors that it could not have known about otherwise. It enables Hamas to communicate with its terrorists in real time to conduct terror attacks. And it enables Hamas to communicate directly with its enemies to intimidate them. Finally, actively engaging Hamas operatives by selectively exposing them to information likely to excite them, Facebook encourages (and profits from) ever-increasing terrorist communication.

This is not merely bad; it is criminal. *E.g.* 18 U.S.C. 2339A, 2339B, 2339C. And it is grounds for liability under the ATA. Facebook can claim no immunity—it actively and intentionally creates all this content. *Accord NFHA* Gov't SOI at 17-24.

[33] *Id.*

### B. Plaintiffs' Claims do Not Seek to Hold Facebook Liable as a Publisher

Section 230 does not immunize anyone for its own tortious *conduct*, only for the *content* of the information it received from another and passively displays. *LeadClick*, 838 F.3d at 176-77 (citing *Accusearch*, 570 F.3d at 1204-05 (Tymkovitch, *J.*, concurring)). As this Court explained, §230 "bars lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions." *Id.* at 174 (cleaned up). The operative question is thus whether "the *duty* that the plaintiff alleges the defendant violated derives from the defendant's status or conduct as a 'publisher or speaker'" so that finding liability "inherently require[s] the court to treat the [defendant] as the 'publisher or speaker'" of content provided by someone else. *Id.* at 175-77 (emphasis added) (quoting *Barnes v. Yahoo!*, 570 F.3d 1096, 1101-02 (9th Cir. 2009)); *Doe*, 824 F.3d at 853 (denying CDA immunity even though defendant's "[p]ublishing activity is a but-for cause" of plaintiff's injuries).

None of plaintiffs' claims asserts a duty that "inherently requires" a court to treat Facebook as a speaker or publisher. Plaintiffs do not attribute the content of any Hamas post to Facebook. Plaintiffs assert a duty to not materially support terrorists. That duty does not vary based on content and does not specifically restrict speech. The ATA, for example, prohibits Walmart from supplying fertilizer, knives, or even food to Hamas. It likewise prohibits Facebook from supplying Hamas a platform and

communications services. Facebook's liability for servicing Hamas is not inherently tied to its status as a speaker or publisher.

Moreover, the word "publisher" refers simply to "one that makes [something] public." *Klayman*, 753 F.3d at 1359.[34] The CDA provides a defense to liability to a defendant that would be "treated as the publisher" of someone else's content. §230(c)(1). It thus requires a showing that the claim would treat the defendant as one that took private information and made it public. Plaintiffs' claims are not dependent on the transformation of information from private to public. By providing services to Hamas, Facebook is liable under the ATA even if it never communicates any of the Hamas postings to anyone not already part of Hamas, and thus never publicizes them. Similarly, Facebook is liable under the ATA even for communicating already-public information. Publication is irrelevant to the ATA.

Finally, none of plaintiffs' claims relates to a publisher's "traditional editorial functions." Facebook's offending activities include facilitating terror networking and targeted communication designed to radicalize by supplying interested people with information that is likely to excite them. That is not due to publication qua publication. Consider this analogy: Suppose an artist wants to sell a painting. He posts a blurb about his painting to his Facebook account. If Facebook were a mere

[34] Black's Law Dictionary first sense of "publish": "To distribute copies (of a work) to the public." Black's Law Dictionary, *publish* (10th ed. 2014).

publisher, like old fashioned Yellow Pages, it would do little more than give the artist a forum, enabling potential buyers to find the artist, perhaps by flipping through the Yellow Pages or searching Google. But Facebook is no mere publisher. Shortly after the artist posts his blurb, Facebook's system analyzes his post and uses its proprietary algorithms to link the artist with other Facebook users who are interested in similar topics. Within minutes, an art collector who posts about his collection on Facebook may learn of the artist's new painting, without doing *anything* to search for it. Facebook determined that the painter and the collector have mutual interests and facilitated or suggested the union of the two. It thus played an active role in facilitating a possible sale. That is matchmaking or brokerage, not publication.

## V. Even if the ATA and §230(c)(1) are in Tension, the ATA Must Control

Because the CDA does not even apply here given that the underlying events all occurred overseas and because, even if applicable, the CDA does not immunize Facebook here, the CDA presents no conflict with the ATA. But even if it did, that conflict would be resolved in favor of the ATA.

### A. Section 230(c)(1) Can Never Apply Against the ATA, Which Civilly Enforces Criminal Counter-Terrorism Provisions

The CDA explicitly disclaims any impact on "enforcement of...any...Federal criminal statute." §230(e)(1). 18 U.S.C. §§2339A, 2339B, & 2339C are all federal

criminal statutes. Thus, the CDA *cannot* provide any immunity for violating those statutes.

Congress intended the ATA, which creates a civil remedy for violations of these criminal statutes, as an important means of depriving terrorists of financial resources and as part of "the growing web of law we are weaving against terrorists." Statement of Alan Kreczko on S. 2465, *supra*. It sees this civil provision as part of the "enforcement" of the predicate criminal statutes mentioned above. *Id.*; S.Rep. 102-342 at 22. Thus, on its terms, the CDA cannot impair enforcement of the ATA.

### B. Expansive Common Law Interpretations of §230(c)(1) Must Yield to the Clear Text of the ATA

Any "conflict" that might exist between §230 and the ATA is due not to the text of §230 but to common law expansions of §230. Section 230 itself grants no immunity. Only judicial decisions applying §230—federal common law—do. Resolving this conflict is simple. Common law deriving from implications of statutory text is abrogated upon a later statutory amendment that alters those implications. *U.S. v. Fausto*, 484 U.S. 439, 453 (1988). Even amendments to *other* statutes that must be read together with the subject statute often effect partial repeal of common law interpreting the latter. "The classic judicial task of reconciling many laws enacted over time, and getting them to make sense in combination, necessarily assumes that the implications of a statute may be altered by the implications of a

later statute." *FDA v. Brown & Williamson*, 529 U.S. 120, 143 (2000) (quotation marks omitted). Thus, if the ATA is inconsistent with common law surrounding §230(c), that common law is abrogated to the extent that it conflicts with the ATA.

### C. Principles of Statutory Interpretation Favor the ATA, the Later-Enacted and More Specific Statute

Assuming the statutory conflict is real, the preferred method of resolving it is to read one or both of the statutes as narrowly as possible to reconcile them, giving effect to both provisions, because Congress presumably intended *both* statutes to be operable. *Ricci v. DeStefano*, 557 U.S. 557, 581 (2009); *New Lamp Chimney v. Ansonia Brass & Copper*, 91 U.S. 656, 662-63 (1875); *SmithKline Beecham v. Watson Pharm.*, 211 F.3d 21, 28 (2d Cir. 2000). It is no option to say that one of the statutes applies "only part of the time." *Schmitt v. Detroit*, 395 F.3d 327, 330 (6th Cir. 2005). When resolving a statutory conflict, "courts have traditionally given weight to statutes' [1] priority of enactment and [2] specificity." *SmithKline*, 211 F.3d at 28 n.3; *In re Ionosphere Clubs*, 922 F.2d 984, 991 (2d Cir. 1990).

Both *SmithKline* factors favor the ATA. *First*, the same Congress that enacted §230 on February 8, 1996,[35] enacted 18 U.S.C. §2339B a few weeks later, on April 24, 1996.[36] Nearly all the individual Members of Congress who voted for §230 also

[35] CDA, Pub. L. 104-104, 110 Stat. 133, 137.

[36] Pub. L. 104-132, 110 Stat. 1247, 1250.

voted for §2339B, and did so *after* enacting §230.[37] If they intended §2339B to have no application in cases involving support for terrorism by interactive computer services, Congress would have said so. It apparently found no conflict. In 2016, Congress enacted JASTA, providing civil litigants "the broadest possible basis...to seek relief against" material supporters of terrorism, 18 U.S.C. 2333, note, further revealing a desire for extraordinarily broad protections for terror victims.

"[A] specific policy embodied in a later federal statute should control our construction of the [earlier] statute, even though it ha[s] not been expressly amended." *Brown & Williamson*, 529 U.S. at 143. The ATA (as amended by JASTA) is the later-enacted statute. The policies it embodies must govern the interpretation of §230(c).

*Second*, the ATA is exceptionally clear and specific. It provides that victims of terrorism may sue any perpetrator or aider and abettor of "international terrorism," a term defined broadly to reference dangerous criminal acts intended to intimidate or coerce. 18 U.S.C. §§2331(1), 2333. It imposes liability on the facts alleged and can be read no other way. It contains no exception for Internet-based claims. In

[37] *Compare* Roll Call Vote 104th Congress, S.735, https://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=104&session=2&vote=00071 (passing §2339B 91-8), *with* Roll Call Vote 104th Congress, S.652, https://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=104&session=2&vote=00008 (passing §230 91-5).

contrast, §230 is non-specific, says nothing of immunity, and requires only that Facebook not be "treated as the publisher or speaker" of the offending posts by third-party terrorists. §230(c)(1). No matter what §230(c) might mean when read while not in conflict with the ATA, once in conflict with the ATA, it *must* be construed narrowly to reconcile it with the ATA. *Ricci*, 557 U.S. 557 at 581.

### D. Alternatively, the Later-Enacted ATA Should Be Deemed to Have Implicitly Repealed §230 to the Extent of the Conflict

Where it is impossible to construe two statutes to avoid irreconcilable conflict, the later-enacted statute is deemed to repeal implicitly the earlier-enacted statute "pro tanto[,] to the extent of the [conflict]." *State of Ga. v. Penn. R.*, 324 U.S. 439, 456-57 (1945); *Cal. Pub. Employees v. WorldCom*, 368 F.3d 86, 104 (2d Cir. 2004).

Section 230(c) was enacted in February 1996 and has not been subsequently amended. The ATA, on the other hand, was amended in 2016 to permit liability for aiding and abetting, an amendment particularly likely to create conflict with §230. 18 U.S.C. §2333(d)(2). If there is an irreconcilable conflict between the ATA and §230, that conflict must be resolved in favor of the later-enacted ATA.

## VI. The District Court's Dramatic Expansion of §230 Yields Absurd Results, Divorces §230 From its Objectives, and Neuters the ATA

The district court held that §230 immunizes Facebook from liability for any claim related to user content. Section 230(c)(1) provides: "No *provider or user* of an

interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." *Id.* (emphasis added). That language requires that providers and users of Internet services be treated with parity. Thus, if Facebook is immune, so too any user who repeats information received from another information content provider. Thus, using the district court's approach, immunity would extend even to a Hamas operative who repeats on Facebook a statement of a Hamas commander (a different "information content provider") calling for terror attacks. It is inconceivable that the Congress that passed the ATA and JASTA intended both to be so significantly subrogated to §230.

That is especially true considering that §230 was enacted to protect children from objectionable material. The decision below transmogrifies §230 into a statute that appears to have been specifically designed to facilitate the spread of terrorism on the Internet. That is precisely the opposite of Congress' intent.

## VII. Choice of Law Rules Prohibit Application of §230 to the Claims Under Israeli Law

New York conflicts law first asks whether the laws at issue "actual[ly] conflict" given the specific facts of the case. *Matter of Allstate*, 81 N.Y.2d 219, 223 (1993); *Finance One Pub. v. Lehman Bros.*, 414 F.3d 325, 331 (2d Cir. 2005). Differences in substantive law create a sufficient conflict where there is "a

'significant *possible* effect on the outcome of the trial.'" *Finance One*, 414 F.3d at 331 (citation omitted) (emphasis in original).

Plaintiffs allege Israeli law claims for 1) negligence under Israel's *Civil Wrongs Ordinance (New Version)—1972* ("CWO") §§35-36; 2) breach of statutory duty under CWO §63; and 3) vicarious liability under CWO §§12 and 15. (129-35).

The elements of negligence in Israel are 1) duty; 2) breach; 3) causation; and 4) damages. *Wultz v. Iran*, 755 F.Supp.2d 1, 57-81 (D.D.C. 2010). Every actor has a duty wherever "a reasonable person ought in the circumstances to have contemplated as likely" that his act or omission will affect another. *Id.* at 57-58. There are two types of duties: subjective "concrete" duty, where an actor, given the facts and circumstances, could have foreseen that his act or omission would yield a harm; and objective "notional" duty, where, as a matter of policy, the actor *ought* to have foreseen the harm (without regard to the particular facts). *Id.* at 58-59.

Although New York negligence law has nominally identical elements, there are significant substantive differences, particularly regarding duty and foreseeability. *See Wultz v. Bank of China*, 811 F.Supp.2d 841, 849-50 (S.D.N.Y. 2011). In Israel, unlike New York, foreseeability and careless conduct can create duty even absent a preexisting duty. *Elmaliach v. Bank of China*, 110 A.D.3d 192, 201 (1st Dep't 2013).

"Breach of statutory duty" under Israeli law (CWO §63) is a civil private right of action for violating any Israeli statute, including penal laws. *Id.* at 67. The Israeli statutes relied on here are *Prevention of Terrorism Ordinance*, 5708-1948, §§1, 4 (prohibiting praise or support of terrorism); Israel's *Penal Law*, 5737-1977, §§134, 136, 144-45, and 148 (banning incitement to violence and material support of terrorism); and Israel's *Defense Regulations (Emergency Period)*, 1945, §§84-85 (prohibiting provision of services to any unlawful organization, including terrorist organizations). New York lacks equivalent law. *Elmaliach*, 110 A.D.3d at 201; *Wultz*, 811 F.Supp.2d at 850.

Although termed "vicarious liability," Israel's CWO §12 differs markedly from American concepts of secondary liability, providing a separate cause of action against a person who participates in, assists, advises, or solicits an act or omission committed or about to be committed by another person, or who orders, authorizes, or ratifies such an act or omission. *Wultz*, 755 F.Supp.2d at 80-81. CWO §15 also recognizes an action against a person for the acts or omissions of a party with whom he contracts if, *inter alia*, he was negligent in selecting the contractor, authorized or ratified the acts of the contractor, or if the contract was entered into for an unlawful purpose. New York lacks a comparable tort. *Elmaliach*, 110 A.D.3d at 201; *Wultz*, 811 F.Supp.2d at 850.

All three claims require conflicts analysis. *Finance One*, 414 F.3d at 332. New York courts employ "interest analysis" to determine which of the competing jurisdictions has the greatest interest in having its tort law applied. *Licci v. Lebanese Canadian Bank*, 672 F.3d 155, 157 (2d Cir. 2012). The analysis distinguishes between "conduct-regulating" rules and "loss-allocating" rules. *Id.* at 158. The relevant Israeli laws on which Plaintiffs base their Israeli causes of action all have regulation of conduct as their primary purpose. *See Devore v. Pfizer*, 58 A.D.3d 138, 141 (1st Dep't 2008). Negligence law is conduct-regulating. *HSA Residential Mortg. v. Casuccio*, 350 F.Supp.2d 352, 364 (E.D.N.Y. 2003). Israel's "breach of statutory duty" claim and the underlying Israeli laws at issue, are designed to uphold statutorily imposed duties to prevent terrorism, violence, and incitement, and to make it harder for terrorists to operate, so are conduct-regulating. So too the "vicarious liability" claim, intended to deter people from participating in, assisting, advising or soliciting another party's tortious acts or omissions.

When a conduct-regulating tort is alleged, "the law of the jurisdiction where the tort occurred will generally apply because that jurisdiction has the greatest interest in regulating behavior within its borders." *Licci*, 672 F.3d at 158. Generally, the "place of the tort" is defined by "the place where the last event necessary to make the actor liable occurred." *Schultz v. Boy Scouts of Am.*, 65 N.Y.2d 189, 197 (1985). That place is Israel. *See Elmaliach*, 110 A.D.3d at 203; *Licci*, 672 F.3d at 158.

Israeli law applies. Facebook's liability attached as a result of events in Israel, where Hamas's attacks occurred and where plaintiffs were injured. Israel also has the strongest interest in this case. *See K.T. v. Dash*, 37 A.D.3d 107, 114 (1st Dep't 2006); *Oveissi v. Iran*, 573 F.3d 835, 842-43 (D.C. Cir. 2009) (when domiciliaries of a particular place are targeted, that place has the greatest interest in having its laws apply). Moreover, by specifically legislating that its anti-terror statutes (on which plaintiffs' "breach of statutory duty" claim is based) apply extraterritorially, Israel has shown strong interest in having its laws apply in cases such as this. *See Wultz*, 755 F.Supp.2d at 68-70.

The district court held that state conflict-of-law rules do not preclude the application of "governing sources of federal law," reasoning that the Supremacy Clause bars application of foreign law contrary to federal law. (419). The district court appears to argue that because state conflicts law makes foreign law applicable, and state conflicts law cannot preempt federal law, the foreign law injected into a case by power of state law cannot preempt federal law. (419). It cites no case for this peculiar argument, justifying it only as required by "logic." (419). But it is illogical as it ignores how the law of conflicts works. Conflicts law is not substantive law; it provides a rule of decision deciding which forum's laws apply. Those substantive laws apply in full. Its purpose is "to assure that a case will be treated [i]n the same way under the appropriate law regardless of the fortuitous circumstances which often

determine the forum." *Lauritzen v. Larsen*, 345 U.S. 571, 591 (1953) (Jackson, *J.*). That purpose would be defeated if some substantive laws of the forum (*i.e.*, federal law) trumped foreign law. Thus, when New York's choice of law rules say to apply Israeli law, Israeli substantive law does not somehow transform into New York law for the purposes of this case. Israeli law applies in full force on its own right.

The Supremacy Clause does not bar the application of foreign law, even if different from federal law. *See id.* at 573, 583-93 (applying Danish substantive law, which was inconsistent with federal statutory law, disposing a claim that would have been valid under federal law). Israeli law applies in full force, subject to its own limitations and defenses, but *not* those substantive defenses provided by federal law. *See id.*

The CDA itself implies the same, expressly preempting "inconsistent" state and local law §230(e)(3), but saying nothing about inconsistent foreign law. By specifically mentioning state law but failing to mention foreign (or simply "all other") law, Congress conveyed that the CDA does not preempt inconsistent foreign law.

## CONCLUSION

For all these reasons, the opinion of the court below should be reversed with instructions that the SAC be accepted as filed and that this case proceed to discovery.

Dated: Baltimore, Maryland
August 23, 2018

Respectfully submitted,

THE BERKMAN LAW OFFICE, LLC
*Attorneys for Plaintiffs-Appellants*

by: /s/ Meir Katz
Meir Katz

Robert J. Tolchin, Esq.
Meir Katz, Esq.
111 Livingston Street, Suite 1928
Brooklyn, New York 11201
(718) 855-3627
RTolchin@berkmanlaw.com
MKatz@berkmanlaw.com

## CERTIFICATE OF COMPLIANCE

Pursuant to FRAP 32(g), I hereby certify that this brief complies with the type-volume limitation of FRAP 32(a)(7)(B) and Circuit Rule 32.1(a)(4)(A), because, excluding the portions of this brief exempted by FRAP 32(f), this brief contains 13,911 words. This word count was made by use of the word count feature of Microsoft Word, which is the word processor used to prepare this brief.

I further certify that this document complies with the typeface requirements of FRAP 32(a)(5) and the type-style requirements of FRAP 32(a)(6).

Dated: Baltimore, Maryland
August 23, 2018

/s/ Meir Katz
Meir Katz
*Attorney for Plaintiffs-Appellants*

**CERTIFICATE OF SERVICE**

I hereby certify that on August 24, 2018, I filed the foregoing using the ECF system, which is expected to electronically serve all counsel of record.

/s/ Meir Katz
Meir Katz

# SPECIAL APPENDIX

## Table of Contents

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------X

RACHELI COHEN, et al.,

Plaintiffs,

-against-

FACEBOOK, INC.,

Defendant.

----------X

STUART FORCE, individually and as Administrator on behalf of the Estate of Taylor Force, et al.,

Plaintiffs,

-against-

FACEBOOK, INC.,

Defendant.

----------X

**MEMORANDUM & ORDER**

**16-CV-4453 (NGG) (LB)**

**16-CV-5158 (NGG) (LB)**

NICHOLAS G. GARAUFIS, United States District Judge.

Plaintiffs in the above-captioned related actions assert various claims against Facebook, Inc. ("Facebook") based on their contention that Facebook has supported terrorist organizations by allowing those groups and their members to use its social media platform to further their aims. The plaintiffs in the first action (the "Cohen Action") are roughly 20,000 Israeli citizens (the "Cohen Plaintiffs"). (Cohen Am. Compl. ("Cohen FAC") (Dkt. 17), No. 16-CV-4453.) The second action (the "Force Action") is brought by victims, estates, and family members of victims of terrorist attacks in Israel (the "Force Plaintiffs" and, together with the Cohen Plaintiffs, "Plaintiffs"). (Force Am. Compl. ("Force FAC") (Dkt. 28), No. 16-CV-5158.)

Before the court are Facebook's motions to dismiss the operative complaints in both actions pursuant to Federal Rules of Civil Procedure 12(b)(1), (2), and (6) (as to the Cohen Action) and 12(b)(2) and (6) (as to the Force Action). (Cohen Def. Mot. to Dismiss ("Cohen MTD") (Dkt. 23), No. 16-CV-4453; Force Def. Mot. to Dismiss ("Force MTD") (Dkt. 34), No. 16-CV-5158.) Because of the substantial similarity in facts and the legal issues raised, the court addresses these motions together in this Memorandum and Order.

For the following reasons, the court GRANTS Facebook's motions to dismiss the operative complaints in both the Cohen Action and the Force Action.

## I. BACKGROUND

### A. Facebook's Social Media Platform

Facebook's eponymous social media website allows users to create personalized webpages that contain information about themselves, including identifying information, photographs, videos, interests, recent activities, and links to content from other websites. (Cohen FAC ¶ 42; see also Force FAC ¶¶ 94-95, 522.) Once a user joins the website, they can engage with other Facebook users in a number of ways, including by adding those users as "friends" and providing feedback to content provided by other users by "sharing," "liking" (i.e. applying a tag that is shared with other users), or commenting on that content. (Cohen FAC ¶ 42; Force FAC ¶ 523.) Additionally, users are able to view their contacts' activities on the website, including both information posted by those contacts as well as their contacts' interactions with other users and content. (See Cohen FAC ¶ 42; Force FAC ¶¶ 524, 527.)

Facebook users are also able to create "groups" with other users, which allows multiple users to join a shared website which has its own profile and information. (Cohen FAC ¶ 43; Force FAC ¶ 525-26.) Members of a group can view, interact with, and share content posted in these group forums. (Cohen FAC ¶ 43.)

Facebook collects data as to its users' activities through the website, including but not limited to information regarding contacts and group associations, content that users post and interact with, and use of third party websites. (Cohen FAC ¶ 44; Force Compl ¶ 528.) Using proprietary algorithms, Facebook generates targeted recommendations for each user, promoting content, websites, advertisements, users, groups, and events that may appeal to a user based on their usage history. (Cohen FAC ¶¶ 45-48; Force FAC ¶¶ 529-41.) In this way, Facebook connects users with other individuals and groups based on projected common interests, activities, contacts, and patterns of usage. (Cohen FAC ¶ 48; Force FAC ¶¶ 530-33.) Facebook also presents users with content posted by other users, groups, and third parties (e.g., advertisers) that is likely to be of interest to them, again based on prior usage history. (Cohen FAC ¶¶ 53-55; Force FAC ¶¶ 534-41.)

**B. The Plaintiffs**

The Cohen Plaintiffs are 20,000 individuals residing in Israel who state that they "have been and continue to be targeted by" attacks by Palestinian terrorist organizations. (Cohen FAC ¶ 4.) The Cohen Plaintiffs claim that they are "presently threatened with imminent violent attacks that are planned, coordinated, directed, and/or incited by terrorist users of Facebook." (Id. ¶ 5.) In particular, they claim to be threatened by an outbreak of violence by Palestinian groups—which they sometimes refer to as the "Facebook Intifada"—and their Complaint recounts 54 separate attacks by Palestinian terrorists and terror groups in Israel since October 1, 2015. (Id. ¶¶ 11-16.)

Unlike the Cohen Plaintiffs, who claim to be threatened only by potential future attacks, the Force Plaintiffs are the estates of victims (and, in one case, the surviving victim) of past attacks by the Palestinian terrorist organization Hamas and the family members of those victims. (Force FAC ¶¶ 5-18). The victims were U.S. citizens, most of whom were domiciled in Israel at

the time of the attacks. (See id.) In their Complaint, the Force Plaintiffs describe the attacks that harmed them, providing a detailed timeline of the events and Hamas's particular involvement in the attacks. (See generally id. ¶¶ 156-499.)

**C. Allegations Against Facebook**

Plaintiffs in the two actions make substantially similar allegations as to Facebook's role in their alleged harms. Plaintiffs claim that Palestinian terrorists[1] "use Facebook's social media platform and communications services to incite, enlist, organize, and dispatch would-be killers to 'slaughter Jews.'" (Cohen FAC ¶ 18; see also Force FAC ¶ 362.) They further aver that Palestinian terrorist groups and associated individuals use their Facebook pages for general and specific incitements to violence and to praise past terrorist attacks. (See Cohen Compl ¶¶ 23-36; Force FAC ¶¶ 111-15.) Plaintiffs allege that Facebook's algorithms, used to connect users with other users, groups, and content that may be of interest to them, play a vital role in spreading this content, as Palestinian terrorist organizations are able to "more effectively disseminate [incitements to violence], including commands to murder Israelis and Jews, to those most susceptible to that message, and who most desire to act on that incitement." (Cohen FAC ¶ 56; see also Force FAC ¶¶ 530-41.)

Plaintiffs allege that Facebook is aware of the use of its platform by Palestinian terrorist organizations and their members but has failed to take action to deactivate their accounts or prevent them from inciting violence. (Cohen FAC ¶ 40; Force FAC ¶ 502-04.) In the case of Hamas, the Force Complaint alleges that Facebook allows that organization, its members, and affiliated organizations to operate Facebook accounts in their own names, despite knowledge that many of them have been officially named as terrorists and sanctioned by various governments.

[1] While the Cohen Complaint refers to Palestinian terrorists and terrorist groups generally, the allegations in the Force Complaint are specific to Hamas, and references to both Complaints together should be read accordingly.

(See Force FAC ¶¶ 118-25.) Plaintiffs claim that Facebook's approach to addressing this use of the platform has been piecemeal (intermittently deleting individual postings or banning users) and inconsistent (e.g., deleting offending posts from one individual without removing identical messages or banning users without taking steps to ensure that the same person does not subsequently rejoin the website under a different moniker). (Id. ¶¶ 549-55; see also Cohen FAC ¶¶ 40, 61-62.)

## II. PROCEDURAL HISTORY

The Cohen Plaintiffs originally filed their action in the Supreme Court of New York, Kings County, and it was removed to this court by Facebook on August 10, 2016, on the basis of diversity of citizenship. (Not. of Removal (Dkt. 1), No. 16-CV-4453.) The operative complaint in this action is the First Amended Complaint, filed on October 10, 2016. (See generally Cohen FAC.) The Cohen Plaintiffs bring Israeli law claims of negligence, breach of statutory duty, and vicarious liability (id. ¶¶ 67-106), as well as New York law claims for prima facie tort, intentional infliction of emotional distress, aiding and abetting a tort, and civil conspiracy (id. ¶¶ 107-34). The Cohen Plaintiffs seek only declaratory and injunctive relief. (Id. ¶¶ 149-55.) Separate from their substantive claims for relief, the Cohen Complaint requests a judicial declaration that the causes of action noted above are not barred by Section 230(c)(1) of the Communications Decency Act, 47 U.S.C. § 230. (Id. ¶¶ 135-48)

The Force Plaintiffs filed their action in the United States District Court for the Southern District of New York on July 10, 2016. (See generally Force Compl. (Dkt. 1), No. 16-CV-5158.) The case was subsequently transferred to this court as related to the Cohen Action on September 16, 2016. (Sept. 16, 2016, Order Reassigning Case (Dkt. 15).) The operative complaint is the First Amended Complaint, filed on October 10, 2016. (Force FAC.) Like the Cohen Complaint, the Force Complaint brings claims for negligence, breach of statutory duty,

and vicarious liability under Israeli law. (Id. ¶¶ 586-620.) The Force Complaint also raises claims under the civil enforcement provisions of the federal Anti-Terrorism Act ("ATA") and the Justice Against Sponsors of Terror Act for aiding and abetting acts of international terrorism, conspiracy in furtherance of acts of international terrorism, and providing material support to terrorist groups in violation of 18 U.S.C. §§ 2339A and 2339B. (Id. ¶¶ 561-85.) The Force Plaintiffs seek $1 billion in compensatory damages, punitive damages to be determined at trial, and treble damages for violations of the federal anti-terrorism statutes. (Id. at ECF p.123.)

## III. DISCUSSION

Before the court are Facebook's motions to dismiss the operative complaints in each of the two actions. (Cohen MTD; Force MTD.) Facebook moves to dismiss the Cohen Complaint for lack of subject matter and personal jurisdiction and for failure to state a claim upon which relief may be granted pursuant to Rules 12(b)(1), (2), and (6) of the Federal Rules of Civil Procedure. (Cohen MTD; see also Mem. in Supp. of Def. Mot. to Dismiss ("MTD Mem.") (Dkt. 24), No. 16-CV-4453.)[2] Facebook separately moves to dismiss the Force Complaint for lack of personal jurisdiction and failure to state a claim upon which relief may be granted pursuant to Rules 12(b)(2) and (6). (Force MTD; see also MTD Mem.)

A court facing challenges as to both its jurisdiction over a party and the sufficiency of any claims raised must first address the jurisdictional question. See Arrowsmith v. United Press Int'l, 320 F.2d 219, 221 (2d Cir. 1963). However, there is no such required ordering as between questions of personal and subject matter jurisdiction. Ruhrgas AG v. Marathon Oil Co., 526 U.S. 574, 586-87 (1999); Carver v. Nassau Cty. Interim Fin. Auth., 730 F.3d 150, 156

[2] The parties briefed the motions to dismiss together, and their filings in support of and opposition to Facebook's motions to dismiss appear in identical form on both the Cohen and Force dockets. In order to avoid confusion, the court's citations to Facebook's Memorandum in Support of the Motions to Dismiss, Plaintiffs' Response in Opposition to the Motions to Dismiss, and Facebook's Reply are to the entries on the Cohen docket.

(2d Cir. 2013) (holding that courts "are not bound to decide any particular jurisdictional question before any other").

The court concludes that the Cohen Plaintiffs lack standing to bring their claims and so dismisses their Complaint in its entirety for lack of subject matter jurisdiction. The court finds that it has personal jurisdiction over Facebook with respect to the claims in the Force Complaint but that the action must be dismissed for failure to state a claim, as Facebook makes out a sufficient affirmative defense pursuant to Section 230(c)(1) of the Communications Decency Act.

**A. Subject Matter Jurisdiction**

Facebook first argues that the Cohen Plaintiffs lack standing to bring their challenges in federal court, as they fail to point to an injury which is either distinguishable from the harm faced by the public at large, fairly traceable to Facebook's actions, or redressable through relief against the company. (See MTD Mem. at 30-32.) The court does not address the potential traceability or redressability issues, as it concludes that the Cohen Plaintiffs do not allege a cognizable "injury-in-fact" and so fail to establish standing.

1. Legal Standard

"A case is properly dismissed for lack of subject matter jurisdiction . . . when the district court lacks the statutory or constitutional power to adjudicate it." Makarova v. United States, 201 F.3d 110, 113 (2d Cir. 2000). "The plaintiff bears the burden of alleging facts that affirmatively and plausibly suggest that it has standing to sue," Cortlandt St. Recovery Corp. v. Hellas Telecomms. S.a.r.l., 790 F.3d 411, 417 (2d Cir. 2015) (internal quotation marks, alterations, and citation omitted), a burden which it must satisfy by a preponderance of the evidence, Luckett v. Bure, 290 F.3d 493, 496-97 (2d Cir. 2002). Courts must "accept as true all material factual allegations in the complaint . . . . [but] jurisdiction must be shown affirmatively,

and that showing is not made by drawing from the pleadings inferences favorable to the party asserting it." Shipping Fin. Servs. Corp. v. Drakos, 140 F.3d 129, 131 (2d Cir. 1998); accord Morrison v. Nat'l Austl. Bank Ltd., 547 F.3d 167, 170 (2d Cir. 2008), aff'd, 561 U.S. 247 (2010).

Federal jurisdiction is constitutionally constrained to "cases" and "controversies," one element of which requires plaintiffs before the court to establish standing: a "genuinely personal stake" in the outcome of a case sufficient to "ensure[] the presence of 'that concrete adverseness which sharpens the presentation of issues upon which [a] court so largely depends.'" Cortland St. Recovery, 790 F.3d at 417 (quoting Baker v. Carr, 369 U.S. 186, 204 (1962)). "In its constitutional dimension, standing imports justiciability," Warth v. Seldin, 422 U.S. 490, 498 (1975), and objections to standing are properly made under Rule 12(b)(1), as they are directed at the court's ability to adjudicate an issue as to parties before it, see, e.g., Tasini v. N.Y. Times Co., 184 F. Supp. 2d 350, 354-55 (S.D.N.Y. 2002).

2. Standing

In order to meet the "irreducible constitutional minimum" of standing, a "plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016) (internal quotation marks and citations omitted). "To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" Id. at 1548 (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)). Additionally, Plaintiffs must demonstrate a "present case or controversy" with respect to claims seeking prospective, injunctive relief, City of L.A. v. Lyons, 461 U.S. 95, 102-03 (1983), and "past injuries cannot satisfy the injury-in-fact requirement" for such claims,

Vaccariello v. XM Satellite Radio, Inc., 295 F.R.D. 62, 72 (S.D.N.Y. 2013) (citing Shain v. Ellison, 356 F.3d 211, 215 (2d Cir. 2004)).

Plaintiffs may, under some circumstances, rely on the risk of a future harm to support their injury in fact, see Deshawn E. v. Safir, 156 F.3d 340, 344 (2d Cir. 1998); however, such injuries are only "actual or imminent" where "the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur."[3] Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334, 2341 (2014) (quoting Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013)). A plaintiff alleging only an "objectively reasonable possibility" that it will sustain the cited harm at some future time does not satisfy this requirement. Clapper, 133 S. Ct at 1147-48. For this reason, courts are generally hostile to "standing theories that require guesswork as to how independent decisionmakers will exercise their judgment," id. at 1150, which almost by definition require speculation as to the likelihood of injury resulting from the third party's actions.

Moreover, plaintiffs cannot evade the required showing of an "actual or imminent" injury by alleging present harms incurred as a result of their "fear[] of a hypothetical future harm that is not certainly impending," as doing so would allow parties to "repackage" their conjectural injury

[3] The Supreme Court's decision in Clapper v. Amnesty International USA emphasized that the "[t]hreatened injury must be 'certainly impending' 'to constitute injury in fact' and 'allegations of possible future injury' are not sufficient. 133 S. Ct. 1138, 1141 (2013). While the Clapper decision acknowledges certain instances in which the Court previously endorsed standing based on a "substantial risk" that the harm would occur if that underlying risk "may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm," id. at 1151 n.5, it appeared to treat those cases as an exception to the general rule. However, the Court's subsequent decision in Susan B. Anthony List v. Driehaus incorporated the "substantial risk" language into its recitation of the standard for measuring injury in fact. 134 S. Ct. 2334, 2341 (2014). At this point, it is not clear when one or the other standard should be applied, see Hedges v. Obama, 724 F.3d 170, 196 (2d Cir. 2013), or even whether those standards are distinct, see N.Y. Bankers Ass'n Inc. v. City of N.Y., No. 13-CV-7212 (KPF), 2014 WL 4435427, at *9 (S.D.N.Y. Sept. 9, 2014). While some courts have applied the potentially lower "substantial risk" analysis in assessing pre-enforcement challenges to laws, such as that considered in Susan B. Anthony List, the governing standard for actuality or imminence with regard to other types of claims is less clear. See, e.g., Hedges, 724 F.3d at 195-96; Knife Rights, Inc. v. Vance, 802 F.3d 377, 384 (2d Cir. 2015). The court need not wade into these questions in the present case. The Cohen Complaint relies wholly on possible future injuries untethered from any allegation as to the likelihood or imminence of their occurrence that are insufficient under either standard.

to "manufacture standing." Id. at 1151. Instead, the focus of the standing inquiry remains whether "the threat creating the fear is sufficiently imminent." Hedges v. Obama, 724 F.3d 170, 195 (2d Cir. 2013); see also Lyons, 461 U.S. at 107 n.8 ("It is the reality of the threat . . . that is relevant to the standing inquiry, not the plaintiff's subjective apprehensions.").

Courts have broadly rejected claims based on the risk of falling victim to a future terrorist attack, concluding that such harms are impermissibly speculative and so insufficient to confer standing. See, e.g., Tomsha v. Gen. Servs. Admin., No. 15-CV-7326 (AJN), 2016 WL 3538380, at *2-3 (S.D.N.Y. June 21, 2016); Bernstein v. Kerry, 962 F. Supp. 2d 122, 127-28 (D.D.C. 2013); People of Colo. ex rel. Suthers v. Gonzales, 558 F. Supp. 2d 1158, 1162 (D. Colo. 2007); cf. George v. Islamic Rep. of Iran, 63 F. App'x. 917, 918 (7th Cir. 2003) (holding that plaintiffs were "no more likely than the average [] citizen to be victims of future attacks" and so their claimed injury was "purely speculative").

3. Application to the Cohen Complaint

The Cohen Plaintiffs fail to carry their burden of showing that their claims are grounded in some non-speculative future harm. Despite offering extensive descriptions of previous attacks (see Cohen FAC ¶¶ 11-16), the Cohen Plaintiffs do not seek redress for past actions but instead seek prospective, injunctive relief based on their allegation that Facebook's actions increase their risk of harm from future terrorist attacks (see, e.g., id. ¶¶ 5, 37). This claimed harm relies on multiple conjectural leaps, most significantly its central assumption that the Cohen Plaintiffs will be among the victims of an as-yet unknown terrorist attack by independent actors not before the court. The Cohen Complaint contains no factual allegation that could form a basis to conclude that those individuals in particular are at any "substantial" or "certainly impending" risk of future harm. Susan B. Anthony List, 134 S. Ct. at 2341. At most, the Complaint shows a general risk of harm to residents of Israel and impliedly asks the court to extract a risk of harm to the Cohen

Plaintiffs based on this risk. Without further allegations, however, the court sees no basis to conclude that the Cohen Plaintiffs "specifically will be the target of any future, let alone imminent, terrorist attack." Tomsha, 2016 WL 3538380, at *2.

Nor can the Cohen Plaintiffs rescue their claims by arguing that they suffer a present harm resulting from their fear of such attacks, as "allegations of a subjective [fear] are not an adequate substitute for a claim of specific present objective harm or threat of a specific future harm." Clapper, 133 S. Ct. at 1152 (quoting Laird v. Tatum, 408 U.S. 1, 13-14 (1972)). While the court does not question the sincerity of the Cohen Plaintiffs' anxieties, their subjective fears cannot confer standing absent a sufficient showing of the risk of future harm.[4]

For the foregoing reasons, the Cohen Complaint is dismissed without prejudice in its entirety. See Carter v. HealthPort Techs., LLC, 822 F.3d 47, 54-55 (2d Cir. 2016) ("[W]here a complaint is dismissed for lack of Article III standing, the dismissal must be without prejudice . . . .").

**B. Personal Jurisdiction**

Facebook also argues that subjecting it to personal jurisdiction in New York as to the Force[5] claims would be inconsistent with state law requirements and due process principles.

---

[4] The Cohen Plaintiffs argue that they establish an injury in fact because "the Israeli statutes [that form the basis for some of their claims] were passed to protect the plaintiffs and impose a duty upon Facebook." (Pls. Mem. in Opp'n to MTD ("Opp'n Mem.") (Dkt. 29), No. 16-CV-4453, at 40.) Their argument appears to be that Israeli law gives rise to a cognizable injury in fact by creating a protected interest. However, the presence of a statutory right does not itself satisfy Article III's injury in fact requirement, which must be met in all cases. See Lujan, 504 U.S. at 576-78. Where, as here, the examining court finds that plaintiffs fail to establish a constitutionally cognizable injury in fact, the resulting jurisdictional defect is not remedied by the presence of a statutory right. See Spokeo, Inc. v. Robbins, 136 S. Ct. 1540, 1549 (2016) ("Article III standing requires a concrete injury even in the context of a statutory violation.").

[5] Facebook's argument against personal jurisdiction is also directed at the Cohen Complaint and raises a number of valid but vexing questions as to the interaction between New York's statutory scheme for extending jurisdiction over corporations and recent Supreme Court decisions concerning due process limitations on personal jurisdiction. (See MTD Mem. at 27-30.) Because the court has determined that the Cohen Plaintiffs fail to establish standing, it need not address the question of personal jurisdiction as to their Complaint. Cf. Ruhrgas AG, 526 U.S. at 583-84 (holding that subject matter questions may be, but are not necessarily, decided before questions of personal jurisdiction).

(See MTD Mem. at 22-30.) The court concludes that personal jurisdiction over Facebook is proper based on the Force Complaint's ATA-based claims, which permit a court to exercise jurisdiction over a defendant who has minimum contacts with the United States, and the doctrine of pendent personal jurisdiction. Accordingly, the court declines to dismiss the Force Complaint on this basis.

1. Legal Standard

Personal jurisdiction refers to a "court's power to exercise control over the parties." Leroy v. Great W. United Co., 443 U.S. 173, 180 (1979). "In order to survive a motion to dismiss for lack of personal jurisdiction, a plaintiff must make a prima facie showing that jurisdiction exists." Licci ex rel. Licci v. Lebanese Canadian Bank, SAL ("Licci III"), 732 F.3d 161, 167 (2d Cir. 2013) (internal quotation marks and citation omitted). "Prior to discovery, a plaintiff may defeat a motion to dismiss based on legally sufficient allegations of jurisdiction." In re Magnetic Audiotape Antitrust Litig., 334 F.3d 204, 206 (2d Cir. 2003) (citation omitted). In evaluating the sufficiency of the jurisdictional allegations, a court must "construe the pleadings and affidavits in the light most favorable to the plaintiffs, resolving all doubts in their favor." Dorchester Fin. Secs. Inc. v. Banco BRJ, S.A., 722 F.3d 81, 85 (2d Cir. 2013) (internal quotation marks and citation omitted).

Establishing personal jurisdiction over a party "requires satisfaction of three primary elements": (1) procedurally proper service of process on the defendant; (2) a statutory basis for personal jurisdiction; and (3) the exercise of jurisdiction must be consistent with "constitutional due process principles." Licci ex rel. Licci v. Lebanese Canadian Bank, SAL ("Licci I"), 673 F.3d 50, 59-60 (2d Cir. 2012). Facebook does not argue that service of process was procedurally improper, and so the court's evaluation focuses on whether the exercise of personal jurisdiction is statutorily authorized and consistent with the strictures of due process.

2. Statutory Basis for Personal Jurisdiction

"The available statutory bases [for asserting personal jurisdiction] are enumerated by Federal Rule of Civil Procedure 4(k)." Licci I, 673 F.3d at 59. In one of its provisions, that rule states that "[s]erving a summons or filing a waiver of service establishes personal jurisdiction over a defendant . . . when authorized by a federal statute." Fed. R. Civ. P. 4(k)(1)(C). Where a federal statute authorizes nationwide service of process, this provision permits the exercise of personal jurisdiction over parties properly served anywhere in the United States. See Kidder, Peabody & Co., Inc. v. Maxus Energy Corp., 925 F.2d 556, 562 (2d Cir. 1991) (stating nationwide service provision of the Securities Exchange Act "confers personal jurisdiction over a defendant who is served anywhere within the United States").

The Force Plaintiffs argue that the service provision of the ATA provides the statutory basis for exercising personal jurisdiction over Facebook. (Pls. Mem. in Opp'n to MTD ("Opp'n Mem.") (Dkt. 29), No. 16-CV-4453, at 7-8). In pertinent part, the relevant statute states that, for civil enforcement of federal antiterrorism statutes pursuant to 18 U.S.C. § 2333, "[p]rocess . . . may be served in any district where the defendant resides, is found, or has an agent."[6] 18 U.S.C. § 2334(a). Various opinions, including two recent decisions from this district, have held that this provision authorizes nationwide service of process and so provides personal jurisdiction over defendants who are properly served anywhere in the United States. Weiss v. Nat'l Westminster Bank PLC, 176 F. Supp. 3d 264, 284 (E.D.N.Y. 2016); Strauss v. Credit Lyonnais, S.A., 175

[6] Immediately before its service provision, Section 2334 states that "[a]ny civil action under section 2333 . . . may be instituted in the district court of the United States for any district where any plaintiff resides or where any defendant resides or is served, or has an agent." 18 U.S.C. § 2334(a). At least one prior opinion restricted nationwide service to instances in which this venue requirement is satisfied. See Wultz v. Islamic Rep. of Iran, 762 F. Supp. 2d 18, 25-29 (D.D.C. 2011). Facebook's apparent concession that it was properly served in the Southern District of New York prior to transfer to this court is also sufficient to establish that statutory venue was proper and so that the statutory prerequisite for nationwide service was satisfied. Cf. Wultz, 762 F. Supp. 2d at 29-30; Weiss v. Nat'l Westminster Bank PLC, 176 F. Supp. 3d 264, 284 n.10 (E.D.N.Y. 2016).

F. Supp. 3d 3, 26-27 (E.D.N.Y. 2016); see also Licci I, 673 F.3d at 59 n.8 (2d Cir. 2012) (noting the ATA's service provision as a potential basis for establishing personal jurisdiction).

Facebook does not argue that service was defective, nor does it contest the holdings in the cases cited above other than to argue that they were wrongly decided. Given the unanimity of opinion on the subject, including within the Second Circuit, and the clear language of the statute, there are no apparent grounds to disagree with Plaintiffs' position. Accordingly, the court finds that the ATA provides statutory grounds for extending personal jurisdiction over Facebook.

3. Due Process Considerations

Even where statutorily authorized, the exercise of personal jurisdiction must be consistent with constitutional due process requirements. See, e.g., Waldman v. Palestine Liberation Org., 835 F.3d 317, 327-28 (2d Cir. 2016). The reviewing court must satisfy itself that "maintenance of a lawsuit does not offend 'traditional notions of fair play and substantial justice.'" Id. at 328 (quoting Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945)).

While the required analysis typically looks to a party's "minimum contacts" with the particular state in which the examining court sits, satisfaction of due process as to federal statutes with nationwide service provisions depends only on a party's contact with the United States as a whole. See, e.g., In re Terrorist Attacks on Sept. 11, 2001, 349 F. Supp. 2d 765, 806 (S.D.N.Y. 2005); cf. Mariash v. Morrill, 496 F.2d 1138, 1143 (2d Cir. 1974) (noting that personal jurisdiction predicated on nationwide service "remains subject to the constraints of the Due Process clause of the Fifth Amendment" (emphasis added)). The First Circuit explained the basis for this distinction, stating: "Inasmuch as the federalism concerns which hover over the jurisdictional equation in a diversity case are absent in a federal question case, a federal court's power to assert personal jurisdiction is geographically expanded." United Elec., Radio, and Mach. Workers of Am. v. 163 Pleasant St. Corp., 960 F.2d 1080, 1085 (1st Cir. 1984).

Applying this reasoning to the ATA's nationwide service provision, courts have consistently held that defendants are subject to personal jurisdiction for civil claims under that act where they have minimum contacts with the United States as a whole.[7] See Waldman, 835 F.3d at 331-334 (assessing personal jurisdiction based on defendants' contacts with the United States as a whole); Strauss, 175 F. Supp. 3d at 28; Weiss, 176 F. Supp. 3d at 285; In re Terrorist Attacks, 349 F. Supp. 2d at 810-11.

There is no question that Facebook has the required contacts with the United States as a whole. The Force Plaintiffs allege—and Facebook does not dispute—that Facebook is incorporated in Delaware and has its principal place of business in California. (Force FAC ¶ 19.) As a United States resident, Facebook could hardly argue that it lacks the required contacts with the country as a whole. Mariash, 496 F.2d at 1143 ("[W]here, as here, the defendants reside within the territorial boundaries of the United States, the 'minimal contacts,' required to justify the federal government's exercise of power over them, are present."); cf. Daimler AG v. Bauman, 134 S. Ct. 746, 760 (2014) (holding that a corporation is "fairly regarded at home" and so "amenable" to personal jurisdiction for suits relating to all of its activities, including those outside the forum, in its principal place of business and place of incorporation). Accordingly, the court finds that exercising of jurisdiction over Facebook with respect to the ATA claims comports with the requirements of due process.

[7] Facebook argues that the ATA cases noted here are distinguishable on the basis that they apply only to foreign defendants, a distinction they claim has legal salience because "any American defendants would have very different federalism-backed expectations than a foreign defendant about where in the United States it may be hailed into court." (Def. Reply in Further Supp. of MTD ("Reply Mem.") (Dkt. 31), No. 16-CV-4453, at 9.) However, Facebook cites no authority that supports this restriction and, though it is correct that analysis of minimum contacts and personal jurisdiction under the ATA has been limited to foreign parties, courts in this circuit have applied the same rule to US-based defendants under other laws with similar provisions. See, e.g., Local 8A-28A Welfare and 401(k) Retirement Funds v. Golden Eagles Architectural Metal Cleaning and Refinishing, 277 F. Supp. 2d 291, 294 (S.D.N.Y. 2003); Hallwood Realty Partners, L.P. v. Gotham Partners, L.P., 104 F. Supp. 2d 279, 281-87 (S.D.N.Y. 2000). Accordingly, the court finds no reasons to treat this distinction as controlling here.

4. Pendent Personal Jurisdiction[8]

"A plaintiff must establish the court's jurisdiction with respect to each claim asserted" Sunward Elec., Inc. v. McDonald, 362 F.3d 17, 24 (2d Cir. 2004), and so the court is required to assess personal jurisdiction as to the Force Complaint's remaining, Israeli law-based claims.

"[U]nder the doctrine of pendent personal jurisdiction, where a federal statute authorizes nationwide service of process, and the federal and [non-federal] claims 'derive from a common nucleus of operative fact', the district court may assert personal jurisdiction over the parties to the related [] claims even if personal jurisdiction is not otherwise available." IUE AFL-CIO Pension Fund v. Herrmann, 9 F.3d 1049, 1056 (2d Cir. 1993) (internal quotation marks and citations omitted). A common nucleus of operative fact exists between claims where "the facts underlying the federal and [non-federal] claims substantially overlap[] [or] the federal claim necessarily [brings] the facts underlying the [non-federal] claim before the court." Achtman v. Kirby, McInerney & Squire, LLP, 464 F.3d 328, 335 (2d Cir. 2006) (internal quotation marks and citation omitted).

District courts have discretion as to whether to exercise pendent personal jurisdiction, the exercise of which should be informed by "considerations of juridical economy, convenience, and fairness to litigants." See In re LIBOR-Based Fin. Instruments Antitrust Litig., No. 11-MD-2262 (NRB), 2015 WL 6243526, at *23 (S.D.N.Y. Oct. 20, 2015) (quoting Oetiker v. Jurid Werke, G.m.b.H., 556 F.2d 1, 5 (D.C. Cir. 1977)).

[8] The Court does not address the potential state law bases for extending personal jurisdiction over the Force Plaintiffs' remaining claims, nor it is required to do so where pendent personal jurisdiction is available. IUE AFL-CIO Pension Fund v. Hermann, 9 F.3d 1049, 1057 (2d Cir. 1993) ("We need not reach the question whether personal jurisdiction as to the state law claims was otherwise available because the district court had personal jurisdiction over the defendants under [a statute with a nationwide service of process provision] and the state law claims derive from a common nucleus of operative facts with the federal claims.")

Those considerations strongly favor exercising pendent jurisdiction over Facebook with respect to the Force Complaint's non-ATA-based claims. The ATA and non-ATA-based claims derive from the same underlying allegations and legal theories: that Facebook's provision of "services" to Hamas assisted that organization in recruiting, organizing, facilitating, and instigating attacks, and that Facebook failed to stop this abuse of its platform. There would be no inconvenience or unfairness to Facebook in requiring it to litigate the same facts before the same court, nor would splitting up the claims between multiple courts do anything to conserve judicial resources. In view of the foregoing discussion of the ATA's nationwide service provision, the court exercises personal jurisdiction over Facebook with respect to the Force Plaintiffs' remaining claims as well.

* * *

Accordingly, the court concludes that Facebook is subject to personal jurisdiction in New York as to the claims asserted in the Force Complaint, and denies its motion to dismiss for lack of personal jurisdiction.

### C. Failure to State a Claim Based on the Communications Decency Act[9]

The parties dedicate much of their briefing debating the applicability of Section 230(c)(1) of the Communications Decency Act ("Section 230(c)(1)") to the present dispute. There are two distinct species of arguments regarding Section 230(c)(1) raised in the parties' briefs. First, the parties dispute whether the asserted claims fall within the substantive coverage of Section 230(c)(1). Second, the Force Plaintiffs argue that Facebook is improperly attempting to apply Section 230(c)(1) extraterritorially. The court considers these arguments separately and

[9] Facebook separately seeks dismissal of the Force Complaint's federal law-based causes of action, arguing that the Force Plaintiffs fail to state a plausible claim for relief under the applicable statutes. (MTD Mem. at 32-40.) The court does not address this argument, as it concludes that all of the Force Complaint's claims must be dismissed on the basis of the Communications Decency Act.

concludes that the activity alleged falls within the immunity granted by Section 230(c)(1) and that application of that subsection to the present dispute is not impermissibly extraterritorial.

1. Legal Standard

The purpose of a motion to dismiss for failure to state a claim under Rule 12(b)(6) is to test the legal sufficiency of a plaintiff's claims for relief. Patane v. Clark, 508 F.3d 106, 112 (2d Cir. 2007). In reviewing a complaint on such a motion, the court must accept as true all allegations of fact, and draw all reasonable inferences in favor of the plaintiff. ATSI Commc'ns, Inc. v. Shaar Fund, Ltd., 493 F.3d 87, 98 (2d Cir. 2007). A complaint will survive a motion to dismiss if it contains "sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007)). However, even where a claim is otherwise plausible, a defendant may move to dismiss based on an available affirmative defense, and the court may grant the motion on that basis "if the defense appears on the face of the complaint." Pani v. Empire Blue Cross Blue Shield, 152 F.3d 67, 74 (2d Cir. 1998); see also Ricci v. Teamsters Union Local 456, 781 F.3d 25, 28 (2d Cir. 2015).

2. Coverage of Section 230(c)(1)

*a. Overview of Section 230(c)(1)*

Section 230(c)(1) shields defendants who operate certain internet services from liability based on content created by a third party and published, displayed, or issued through the use of the defendant's services. That subsection states: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1).

The Second Circuit recently described the necessary components of an immunity claim under Section 230(c)(1), stating that the law "shields conduct if the defendant (1) is a provider or

user of an interactive computer service, (2) the claim is based on information provided by another information content provider and (3) the claim would treat [the defendant] as the publisher or speaker of that information." FTC v. LeadClick Media, LLC, 838 F.3d 158, 173 (2d Cir. 2016) (alteration in original) (internal quotation marks and citations omitted). Where a defendant establishes these requirements based on the face of a complaint, a motion to dismiss may be granted. See Ricci, 781 F.3d at 28 (citing Klayman v. Zuckerberg, 753 F.3d 1354, 1357 ("Klayman II") (D.C. Cir. 2014)).

The Force Plaintiffs do not genuinely contest that the first and second elements of this test are satisfied in the present case,[10] but rather focus their efforts on contesting the final requirement for obtaining Section 230(c)(1) immunity—that "the claim would treat [the defendant] as the publisher or speaker of" third party content. Under this prong, qualifying defendants are protected from liability predicated on their "exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone, or alter content" that they did not themselves create. LeadClick Media, 838 F.3d at 174 (internal quotation marks and citation omitted). The Second Circuit's most recent opinion on the subject provided the following guidance as to when a defendant is shielded:

> [W]hat matters is whether the cause of action inherently requires the court to treat the defendant as the "publisher or speaker" of content provided by another. To put it another way, courts must ask whether

[10] While the court does not engage in an extended discussion of the first two prongs here, Facebook and the content at issue qualify easily. The Second Circuit has not considered whether social media platforms in particular are "interactive computer services" within the meaning of the law; however, other courts have readily concluded that such websites (and Facebook in particular) fall into this category. See, e.g., Klayman II, 753 F.3d at 1357-58; Doe v. MySpace, Inc., 528 F.3d 413, 420-22 (5th Cir. 2008). With regard to the second prong—that the "claim is based on information provided by another content provider"—the Second Circuit has indicated that a defendant falls afoul of this requirement only where "it assisted in the development of what made the content unlawful." LeadClick Media, 838 F.3d at 174. The District Court for the District of Columbia recently rejected an argument that Facebook fell afoul of this standard by using data collected from users to suggest other content and users, stating that "the manipulation of information provided by third parties does not automatically convert interactive service providers into information content providers." Klayman v. Zuckerberg, 910 F. Supp. 2d 314, 321 n.3 ("Klayman I") (D.D.C. 2012), aff'd, 753 F.3d 1354 (D.C. Cir. 2014).

> the duty that the plaintiff alleges the defendant violated derives from the defendant's status or conduct as a "publisher or speaker."

Id. at 175 (quoting Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1102 (9th Cir. 2009)) (emphasis added). This guidance emphasizes that Section 230(c)(1) is implicated not only by claims that explicitly point to third party content but also by claims which, though artfully pleaded to avoid direct reference, implicitly require recourse to that content to establish liability or implicate a defendant's role, broadly defined, in publishing or excluding third party communications. See, e.g., Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12, 19 (1st Cir. 2016) ("The ultimate question [of whether Section 230(c)(1) applies] does not depend on the form of the asserted cause of action . . . .") (collecting cases); Manchanda v. Google, No. 16-CV-3350 (JPO), 2016 WL 6806250, at *2 (S.D.N.Y. Nov. 16, 2016).

In keeping with this expansive view of the publisher's role, judicial decisions in the area consistently stress that decisions as to whether existing content should be removed from a website fall within the editorial prerogative. See Ricci, 781 F.3d at 28; Klayman II, 753 F.3d at 1359; Green v. Am. Online (AOL), 318 F.3d 465, 471 (3d Cir. 2003) ("[D]ecisions relating to the monitoring, screening, and deletion of content from [defendant's] network . . . quintessentially relate[] to a publisher's role."); Barnes, 570 F.3d at 1103 ("[R]emoving content is something publishers do."). Similarly, a recent opinion found that decisions as to the "structure and operation" of a website also fall within Section 230(c)(1)'s protection, Backpage.com, 817 F.3d at 21, a determination which one court extended to a social media platform's decisions as to who may obtain an account, see Fields v. Twitter, -- F. Supp. 3d --, No. 16-CV-213, 2016 WL 6822065, at *6 ("Fields II") (N.D. Cal. Nov. 18, 2016).

*b. Application*

While the Force Plaintiffs attempt to cast their claims as content-neutral, even the most generous reading of their allegations places them squarely within the coverage of Section 230(c)(1)'s grant of immunity. In their opposition to the present motion, the Force Plaintiffs argue that their claims seek to hold Facebook liable for "provision of services" to Hamas in the form of account access "coupled with Facebook's refusal to use available resources . . . to identify and shut down Hamas [] accounts." (Opp'n Mem. at 27; see also Force FAC ¶¶ 543-55.) While superficially content-neutral, this attempt to draw a narrow distinction between policing accounts and policing content must ultimately be rejected. Facebook's choices as to who may use its platform are inherently bound up in its decisions as to what may be said on its platform, and so liability imposed based on its failure to remove users would equally "derive[] from [Facebook's] status or conduct as a 'publisher or speaker.'" LeadClick Media, 838 F.3d at 175 (internal quotation marks and citations omitted). Section 230(c)(1) prevents courts from entertaining civil actions[11] that seek to impose liability on defendants like Facebook for allowing third parties to post offensive or harmful content or failing to remove such content once posted. See Ricci, 781 F.3d at 28; Klayman II, 753 F.3d at 1359 ("[T]he very essence of publishing is making the decision whether to print or retract a given piece of content."). For the same reason, it is clear that Section 230(c)(1) prevents the necessarily antecedent editorial decision to allow

[11] The Force Plaintiffs also refer in passing to a subsection of Section 230 which states that "[n]othing in this section shall be construed to impair the enforcement of . . . any [] Federal criminal statute." 47 U.S.C. § 230(e)(1). (Opp'n Mem. at 26-27.) While, read most favorably, this section could be interpreted to inhibit immunity as to civil liability predicated on federal criminal statutes, such as the ATA provisions at issue here, this reading has been rejected by most courts that have examined it. See Backpage.com, 817 F.3d at 23; M.A. ex rel P.K. v. Vill. Voice Media Holdings, LLC, 809 F. Supp. 2d 1041, 1054-55 (E.D. Mo. 2011); Doe v. Bates, No. 5:05-CV-91, 2006 WL 3813758, at *3-4 (E.D. Tex. Dec. 27, 2006); Obado v. Magedson, No. 13-cv-2382, 2014 WL 3778261 (D.N.J. July 31, 2014); but see Nieman v. Versuslaw, Inc., No.12-3104, 2012 WL 3201931, at *9 (C.D. Ill. Aug. 3, 2012). The court concludes that this subsection does not limit Section 230(c)(1) immunity in civil actions based on criminal statutes but rather extends only to criminal prosecutions.

certain parties to post on a given platform, as that decision cannot be meaningfully separated from "choices about what [third party] content can appear on [the platform] and in what form." Fields II, 2016 WL 6822065, at *6 (quoting Backpage.com, 817 F.3d at 20-21).

Further, it is clear that the Force Plaintiffs' claims are not based solely on the provision of accounts to Hamas but rely on content to establish causation and, by extension, Facebook's liability. The essence of the Force Complaint is not that Plaintiffs were harmed by Hamas's ability to obtain Facebook accounts but rather by its use of Facebook for, inter alia, "recruiting, gathering information, planning, inciting, [] giving instructions for terror attacks, . . . issu[ing] terroristic threats, . . . [and] intimidating and coerc[ing] civilian populations." (Force FAC ¶ 112; see also Opp'n Mem. at 29 ("[P]laintiffs have alleged how Facebook's provision of services and resources to Hamas substantially contributed to Hamas's ability to carry out the attacks at issue and the attacks were a foreseeable consequence of the support provided by Facebook.") Said differently, the Force Plaintiffs claim that Facebook contributed to their harm by allowing Hamas to use its platform to post particular offensive content that incited or encouraged those attacks. Facebook's role in publishing that content is thus an essential causal element of the claims in the Force Complaint, and allowing liability to be imposed on that basis would "inherently require[] the court to treat the defendant as the publisher or speaker of content provided by" Hamas. LeadClick Media, 838 F.3d at 175 (internal quotation marks and citations omitted); see also Fields II, 2016 WL 6822065, at *7 ("Although plaintiffs have carefully restructured their [complaint] to focus on their provision of accounts theory of liability, at their core, plaintiffs' allegations are still that [the social media platform] failed to prevent [terrorists] from disseminating content through [its] platform, not its mere provision of accounts . . . .").

Accordingly, the court finds that the Force Plaintiffs' claims against Facebook fall within the scope of Section 230(c)(1)'s grant of immunity. The court proceeds to consider whether that statute may be applied to the present dispute.

3. Extraterritorial Application of the Communications Decency Act

Separate from its substantive scope, the Force Plaintiffs argue that Section 230(c)(1) does not apply to the present dispute because, under the presumption against extraterritoriality, it cannot be applied to conduct that occurs wholly outside of the United States. (See Opp'n Mem. at 30-31.) Pointing to recent Supreme Court holdings, Plaintiffs claim that because "the CDA 'gives no clear indication of an extraterritorial application,' under [Morrison v. Nat'l Austl. Bank Ltd., 561 U.S 247 (2010)], the CDA has no extraterritorial application." (Id. at 31.)

*a. Overview of the Presumption against Extraterritoriality*

Based on the premise that "United States law governs domestically but does not rule the world," the presumption against extraterritoriality dictates that statutes should only be given domestic effect absent a definitive demonstration of Congress's intent for them to apply abroad. See RJR Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090, 2100 (2016) (internal quotation marks and citations omitted). While "the presumption against extraterritoriality is 'typically' applied to statutes 'regulating conduct,'" id. at 2100 (quoting Kiobel v. Royal Dutch Petroleum, 133 S. Ct. 1659, 1664 (2013)), the Supreme Court recently clarified that, "regardless of whether the statute in question regulates conduct, affords relief, or merely confers jurisdiction," all questions of extraterritoriality should be assessed using a "two-step framework," id. at 2101.

The first step requires the court to determine "whether the statute gives a clear, affirmative indication that it applies extraterritorially." Id. The presumption against extraterritoriality does not apply if a statute contains an express demonstration of Congress's intent that the law should apply abroad. See Morrison, 561 U.S. at 255. Conversely, absent

evidence of such intent, the statute can only be applied domestically. Id. ("[W]hen a statute gives no clear indication of extraterritorial application, it has none.")

If a statute lacks clear indicia of intended extraterritorial effect, the examining court must then "determine whether the case at issue involves [] a prohibited [extraterritorial] application" of the law. Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp. ("Microsoft Corp."), 829 F.3d 197, 216 (2d Cir. 2016). Accomplishing this step requires the court to identify the "focus" of the statute, defined as the "objects of the statute's solicitude." Morrison, 561 U.S. at 267. From this, the court must distill the relevant "territorial events or relationships" that bear on that "focus," see Microsoft Corp. at 216 (internal citation omitted), separating those events whose location is relevant to the statute's central emphasis from those that are peripheral. The final element of this analysis requires the court to assess whether the relevant "territorial events and relationships" occurred domestically or abroad with respect to the challenged application of the statute. Id. If, in the final analysis, the court determines that "the domestic contacts presented by the case fall within the 'focus' of the statutory provision or are 'the objects of the statute's solicitude,' then the application of the provision is not unlawfully extraterritorial." Id. (quoting Morrison, 561 U.S. at 267).

*b. Application to Section 230(c)(1)*

i. Indicia of Section 230(c)(1)'s Intended Extraterritorial Effect

No other court appears to have addressed the presumption against extraterritoriality in the context of a statute which limits liability or imparts immunity. At the outset, the court agrees with the Force Plaintiffs that the statute itself lacks an "affirmative indication that it applies extraterritorially," RJR Nabisco, 136 S. Ct. at 2101, as none of Section 230(c)(1), the surrounding provisions, or any other section of the Communications Decency Act demonstrate

any clear consideration of such application, see Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 56, §§ 501-61 (codified in scattered sections of Title 18 and Title 47 of the United States Code).

ii. Determining the Statutory "Focus"

Moving on to find the statute's "focus," the court concludes that the "object[] of [Section 230(c)(1)'s] solicitude" is its limitation on liability. Morrison, 561 U.S. at 267. In drawing this conclusion, the court turns "to the familiar tools of statutory interpretation," Microsoft Corp., 829 F.3d at 217, determining the relevant provision's focus by examining its text and context.

Looking first to the plain language of Section 230(c)(1), the court concludes that the "most natural reading of [that provision] . . . suggests a legislative focus on" providing immunity. Id. Section 230(c)(1) offers only one directive—that qualifying defendants may not be treated as the "publisher or speaker of any" third party content—which it does not cabin based on either the location of the content provider or the user or provider of the interactive computer service. 47 U.S.C. § 230(c)(1). This emphasis on immunity over other considerations is clear from the text, and courts interpreting that provision have consistently found Section 230(c)(1)'s plain language focuses on protecting qualified defendants from civil suits. See, e.g., Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997).

Viewing the relevant language in the context of the surrounding provisions and the policy goals of that section further supports this view of its "focus." Other than the relevant provision, Section 230 contains only two other substantive provisions, one of which is similarly explicit in

limiting civil liability for providers and users of interactive computer services.[12] 47 U.S.C. § 230(c)(2). Both of these immunizing provisions were adopted specifically for the purpose of clarifying—and curtailing—the scope of internet-providing defendants' exposure to liability predicated on third party content,[13] and much of the surrounding statutory language emphasizes and supports this focus. This is evidenced, for instance, by Section 230's stated purpose of preserving an open and free internet uninhibited by external limitations, see 47 U.S.C. § 230(b)(2), and its listed exceptions to the broad liability provided therein, see id. § 230(e).

iii. Ascertaining the Relevant "Territorial Events and Relationships"

In light of its focus on limiting civil liability, the court concludes that the relevant location is that where the grant of immunity is applied, i.e. the situs of the litigation. Section 230(c)(1) suggests a number of "territorial relationships and events," which are generally divisible into those associated with the underlying claim (e.g., the location of the information content provider, the internet service provider, or the act of publishing or speaking) and the location associated with the imposition of liability, i.e. where the internet service provider is to

[12] Section 230 also requires interactive computer service providers to provide notice to customers of commercially available parental control products that allow for content limitations. 47 U.S.C. § 230(d).

[13] Notes of debates around the adoption of the precise language at issue demonstrate that Congress acted with the purpose of limiting liability. See H.R. Rep. No. 104–458, at 194 (1996) (H.R. Conf. Rep.), reprinted in 1996 U.S.C.C.A.N. 10. The court observes, however, that the legislative intent is not unequivocal in this regard. The provision at issue was adopted in response to a New York case, Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), which held an internet service provider liable for the comments by its users, concluding that the service provider became a "publisher" by virtue of having selectively removed content and so was subject to liability for republishing defamatory comments that it had not removed. Id. at *3-4. In overruling that decision, Congress evidently sought to remove disincentives to selective removal of material created by that opinion, which it concluded would impair "the important federal policy of empowering parents to determine the content of communications their children receive through interactive computer service." H.R. Rep. No. 104–458 at 194. Some opinions have noted that the subsequent interpretation of the law, which arguably undermines information service providers' incentives to remove any information by inculcating them against liability for the content they display, overreads the protections that Congress sought to provide. See Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. craigslist, Inc., 519 F.3d 666, 669-70 (7th Cir. 2008). Whatever the merits of that argument, for present purposes it is relevant only to show that Congress's "focus" in including the relevant language was on limiting liability, not its reasons for adopting that policy.

be "treated" as the publisher or speaker. Given the statutory focus on limiting liability, however, the location of the relevant "territorial events" or "relationships" cannot be the place in which the claims arise but instead must be where redress is sought and immunity is needed.

With this in mind, the court concludes that the Force Action does not require an impermissible extraterritorial application of Section 230(c)(1). As the situs of the litigation is New York, the relevant "territorial events or relationships" occur domestically. Accordingly, the court rejects the Force Plaintiff's argument that Facebook should be denied immunity under Section 230(c)(1).[14]

* * *

Accordingly, the court grants Facebook's motion to dismiss all claims in the Force Complaint for failure to state a claim upon which relief can be granted.

[14] The Force Plaintiffs separately claim that Section 230(c)(1) does not apply to claims based in foreign law (Opp'n Mem. at 31), and argue that their Israeli tort law claims are properly before the court under a conflict of laws analysis (id. at 31-36). Their argument that the Communications Decency Act does not limit Israeli law claims is apparently based on lack of any reference to foreign law in the Section 230's subsection entitled "Effect on other laws." 47 U.S.C. § 230(e). The relevant subsection provides a limited list of exceptions to Section 230(c)'s limitations on liability. See, e.g., id §§ 230(e)(1) (stating that the liability provisions do not impair enforcement of federal criminal laws), 230(e)(3) (stating that Section 230 does not affect state laws that are "consistent with this section"). The Force Plaintiffs argue that failing to include foreign law in this section indicates that Section 230(c)(1)'s grant of immunity does not apply to Israeli law-based claims. The court disagrees and understands the significance of this omission to be just the opposite: because there is no listed exception for foreign law claims, those claims remain subject to the limitations on liability provided by Section 230(c)(1). Cf. TRW Inc. v. Andrews, 534 U.S. 19, 28 (2001) ("Where Congress explicitly enumerates certain exceptions to a general prohibition, additional exceptions are not to be implied, in the absence of evidence of a contrary legislative intent." (internal quotation marks and citations omitted)).

## IV. CONCLUSION

For the foregoing reasons, Facebook's Motions to Dismiss ((Dkt. 23), No. 16-CV-4453; (Dkt. 34), No. 16-CV-5158) are GRANTED. The Amended Complaint in the Cohen Action (Dkt. 17), No. 16-CV-4453) is DISMISSED WITHOUT PREJUDICE. The Amended Complaint in the Force Action ((Dkt. 28), No. 16-CV-5158) is DISMISSED WITHOUT PREJUDICE. The Clerk of Court is respectfully DIRECTED to enter judgment accordingly.

SO ORDERED.

s/Nicholas G. Garaufis

Dated: Brooklyn, New York
May 18, 2017

NICHOLAS G. GARAUFIS
United States District Judge

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------X

RACHELI COHEN, et al.,

Plaintiffs,

-against-

FACEBOOK, INC.,

Defendant.

----------X

JUDGMENT
16-CV- 4453 (NGG)

STUART FORCE, individually and as Administrator on behalf of the Estate of Taylor Force, et al.,

Plaintiffs,

-against-

FACEBOOK, INC.,

Defendant.

----------X

16-CV- 5158 (NGG)

A Memorandum and Order of Honorable Nicholas G. Garaufis, United States District Judge, having been filed on May 18, 2017, granting Facebook's motions to dismiss ((Dkt.23), No. 16-CV-4453 and (Dkt. 34), No. 16-CV-5158); dismissing the Amended Complaint in the Cohen Action (Dkt.17), No. 16-CV-4453) without prejudice; and dismissing the Amended Complaint in the Force Action ((Dkt. 28), No. 16-CV-5158) without prejudice; it is

ORDERED and ADJUDGED that Facebook's motions to dismiss No. 16-CV-4453 and No. 16-CV-5158 are granted; that the Amended Complaint in the Cohen Action No.

**JUDGMENT** 16-CV-5158 (NGG)

16-CV-4453 is dismissed without prejudice; and that the Amended Complaint in the Force

Action No. 16-CV-5158 is dismissed without prejudice.

Dated: Brooklyn, New York
May 18, 2017

Douglas C. Palmer
Clerk of Court

by: */s/ Janet Hamilton*
Deputy Clerk

D/F

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

STUART FORCE, individually and as Administrator on behalf of the Estate of Taylor Force, et al.,

Plaintiffs,

-against-

FACEBOOK, INC.,

Defendant.
----------X

**MEMORANDUM & ORDER**

**16-CV-5158 (NGG) (LB)**

NICHOLAS G. GARAUFIS, United States District Judge.

Plaintiffs in the above-captioned action are the victims, estates, and family members of victims of terrorist attacks in Israel. (1st Am. Compl. ("FAC") (Dkt. 28).) They assert various claims against Facebook, Inc. ("Facebook") based on their contention that Facebook has supported the terrorist organization Hamas by allowing that group and its members and supporters to use Facebook's social media platform to further their aims.

On May 18, 2017, the court dismissed Plaintiffs' first amended complaint without prejudice for failure to state a claim upon which relief may be granted.[1] (May 18, 2017, Mem. & Order ("May 18 M&O") (Dkt. 48).) Before the court are Plaintiffs' motions to alter the judgment dismissing the first amended complaint (Mot. to Alter J. ("Recons. Mot.") (Dkt. 50)) and for leave to file a second amended complaint (Mot. for Leave to File 2d Am. Compl. ("Amendment Mot.") (Dkt. 52)). For the following reasons, the court DENIES both motions.

[1] In that order, the court also addressed the factually similar allegations in Cohen v. Facebook, Inc., No. 16-CV-4453, and dismissed the operative complaint in that case as well. (May 18 M&O.)

## I. BACKGROUND

The court assumes familiarity with Plaintiffs' allegations and the court's prior decision granting Facebook's motion to dismiss Plaintiffs' first amended complaint. (See May 18 M&O.) In that opinion, the court specified that the dismissal was without prejudice. (Id. at 28.) On June 15, 2017, Plaintiffs filed two motions: first, a motion to alter the judgment, "retracting [the May 18 M&O] and issuing a modified opinion denying Facebook's motion to dismiss" (Recons. Mot.); and second, a motion for leave to file a second amended complaint, a copy of which Plaintiffs appended to their memorandum in support of that motion (Amendment Mot.; see also Proposed 2d Am. Compl. ("PSAC") (Dkt. 53-1)).

## II. DISCUSSION

### A. Motion to Alter the Judgment

Plaintiffs ask the court to reconsider its dismissal of the first amended complaint. The court concluded that all of the claims contained therein were barred by Section 230(c)(1) ("Section 230") of the Communications Decency Act ("CDA"), 47 U.S.C. § 230(c)(1). That law states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1). Examining the myriad opinions considering the application of that law, the court concluded that each of Plaintiffs' claims and theories of liability sought to hold Facebook liable based on its role as the "publisher or speaker" of social media content generated by Hamas and affiliated individuals, and so were barred by the defense afforded by Section 230. (May 18 M&O at 17-23.) The court also held that applying Section 230 to the claims and theories at issue did not require an impermissible extraterritorial application of the CDA, as the relevant location for its extraterritoriality analysis was "the situs of the litigation." (Id. at 26.)

Plaintiffs contend that the court erred both in its determination that Section 230 applied to the claims raised in the first amended complaint and that the application of that law to those claims was not impermissibly extraterritorial. They seek reconsideration and rescission of the opinion dismissing their complaint pursuant to Rule 59(e) of the Federal Rules of Civil Procedure. For the reasons that follow, the court sees no reason to reconsider its previous decision dismissing the first amended complaint.

1. Legal Standard

"A motion for reconsideration should be granted only when the [moving party] identifies 'an intervening change of controlling law, the availability of new evidence, or the need to correct a clear error or prevent manifest injustice.'" Kolel Beth Yechiel Mechil of Tartikov, Inc. v. YLL Irrevocable Tr., 729 F.3d 99, 104 (2d Cir. 2013) (quoting Virgin Atl. Airways v. Nat'l Mediation Bd., 956 F.2d 1245, 1255 (2d Cir. 1992)). "It is well-settled that Rule 59 is not a vehicle for relitigating old issues, presenting the case under new theories, securing a rehearing on the merits, or otherwise taking a 'second bite at the apple.'" Analytical Surveys, Inc. v. Tonga Partners, L.P., 684 F.3d 36, 52 (2d Cir. 2012) (internal quotation marks and citation omitted). "[T]he standard for granting a Rule 59 motion for reconsideration is strict, and reconsideration will generally be denied unless the moving party can point to controlling decisions or data that the court overlooked." Id. (quoting Shrader v. CSX Transp., Inc., 70 F.3d 255, 257 (2d Cir. 1995)) (alterations omitted). "The burden is on the movant to demonstrate that the Court overlooked controlling decisions or material facts that were before it on the original motion and that might materially have influenced its earlier decision." Schoolcraft v. City of New York, 248 F. Supp. 3d 506, 508 (S.D.N.Y. 2017); see also Levin v. Gallery 63 Antiques Corp., No. 04-CV-1504 (KMK), 2007 WL 1288641, at *2 (S.D.N.Y. Apr. 30, 2007) ("Motions for reconsideration allow

the district court to correct its own mistakes, not those of the Parties." (internal quotation marks and citations omitted)).

2. Application

Plaintiffs argue that the court erred in (1) determining that the "focus" of Section 230 was on the "limitation of liability;" and (2) applying Section 230 to the claims against Facebook and, particularly, to claims raised under the Anti-Terrorism Act ("ATA") and Israeli law. (See generally Mem. in Supp. of Mot. for Recons. ("Recons. Mem. (Dkt. 51).) The court addresses these arguments in turn.

*a. "Focus" of Section 230*

Plaintiffs first argue that the court erred in concluding that the presumption against extraterritoriality did not preclude application of Section 230 to the allegations raised in the first amended complaint. Plaintiffs take particular issue with the court's determination that Section 230's "focus" was on that section's "limitation on liability." (Recons. Mem. at 4 (quoting May 18 M&O at 25).) Plaintiffs argue both that the court's identification of the statutory "focus" was based on an overly narrow focus on the provision at issue in this litigation, Section 230(c)(1) (Recons. Mem. at 4-5), and that the court's conclusion that the statute's focus is on liability "wrongly conflates the effect of a statute with its focus," which is on the actions of interactive computer providers (id. at 5-8).

Plaintiffs' arguments on this point do not come close to meriting reconsideration. The court notes that Plaintiffs at no point attempted to raise either of these arguments in their opposition to Facebook's motion to dismiss; in fact, the portions of Plaintiffs' brief discussing extraterritoriality do not even mention the word "focus." (See Pls. Mem. in Opp'n to Mot. to Dismiss ("Pls. MTD Opp'n") (Dkt. 40) at 30-31.) Plaintiffs provide no reason why they could not have presented such arguments in their initial briefing, and such new arguments have no

place in a motion for reconsideration. See, e.g., Schoolcraft, 248 F. Supp. 3d at 508. While Plaintiffs now seek to take a new tack, "[a] party requesting reconsideration is not supposed to treat the court's initial decision as the opening of a dialogue in which that party may then use Rule [59(e)] to advance new facts and theories in response to the court's rulings." Id. at 509 (quoting Church of Scientology Int'l v. Time Warner, Inc., No. 92-CV-3024 (PKL), 1997 WL 538912, at *2 (S.D.N.Y. Aug. 27, 1997)).

Moreover, Plaintiffs identify no contrary authority that the court overlooked or misapplied, as is normally required to obtain reconsideration. See Analytical Surveys, 684 F.3d at 52. Instead, Plaintiffs contend the court's approach is generally at odds with Supreme Court and Second Circuit opinions examining issues of extraterritoriality because the court failed to adequately account for "statutory context." (Recons. Mem at 4-6.) Plaintiffs plainly misread the court's opinion, however, which was explicit in basing its conclusion about the statute's focus on its reading of Section 230 as a whole. (See May 18 M&O at 25-26 (examining policy statements and substantive provisions of Section 230).)

Plaintiffs' second argument—that the court's holding that Section 230's focus is on limiting liability "wrongly conflates the effect of a statute with its focus" (Recons. Mem. at 6-7)—is likewise unsupported by any contrary authority. Plaintiffs wave their hands at two recent Supreme Court decisions contemplating statutes other than the CDA and purport to draw from those decisions the proposition that "no statute's focus can ever be to simply limit liability." (Id. at 6-7 (citing Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247 (2010), and Kiobel v. Royal Dutch Petroleum Co., 569 U.S. 108 (2013)).) However, those decisions offer no support for such a broad generalization, as they examine only the particular statutes before the Court while stressing that the touchstone of extraterritoriality analysis must be on the "focus of congressional

concern" in enacting the challenged statute. Morrison, 561 U.S. at 266. The court sees nothing in those opinions that disturbs its analysis of the CDA and certainly sees nothing that suggests that Congress's focus in enacting a statute can never be on limiting liability.

*b. The Scope of the CDA*

Plaintiffs next argue that the court misapplied Section 230 to their claims against Facebook. (Recons. Mem. at 8-17.) Plaintiffs make two separate arguments: first, that the court failed to consider Plaintiffs' allegations and arguments that Facebook acted as an "information content provider," independent of content provided by Hamas-affiliated users (id. at 11-14); and second, that the court incorrectly extended Section 230's coverage to "valuable services" provided by Facebook (id. at 14-17). The court examines these arguments separately.

i. Facebook's Role as "Information Content Provider"

Plaintiffs first contend that the court failed to address their contention that Facebook acted as an "information content provider" within the meaning of Section 230 and could not claim protection under that section. As noted in the court's original decision, the protection afforded by Section 230 applies only to claims "based on information provided by [an] information content provider" other than the defendant. (May 18 M&O at 18-19 (quoting FTC v. LeadClick Media, LLC, 838 F.3d 158, 173 (2d Cir. 2016)).) Plaintiffs now maintain that their claims have, in fact, always sought to hold Facebook liable for its own content, and not that generated by another "information content provider," i.e. Hamas and related entities, based on Facebook's alleged role in "networking" and "brokering" links among terrorists. (Recons. Mot. at 12.)

Plaintiffs' contention is completely disingenuous. In the current motion, Plaintiffs acknowledge in a footnote that "perhaps plaintiffs could have made their reliance on Facebook's productive conduct clearer in their briefing" but attribute this oversight to Facebook's supposed

failure to argue that it was not a content provider. (Recons. Mot. at 12 & n.9.) Plaintiffs' contention is flatly refuted by Facebook's briefing on the original motion to dismiss, which clearly argued that all of the offending content cited in Plaintiffs' complaint was "provided by another information content provider, not by Facebook itself." (Def. Mem. in Supp. of MTD (Dkt. 35) at 17-18.) Plaintiffs did not respond to this argument at any point, and in fact began their opposition memorandum by stating that "[t]hese cases do not concern speech or content." (Pls. MTD Opp'n at 1.) For Plaintiffs to now turn around and argue that its allegations are largely about content that Facebook itself created borders on mendacious. More to the point, this entirely new argument in support of liability is not suitably considered on a motion for reconsideration, which "may not be used to advance new facts, issues or arguments not previously presented to the Court." See Montblanc-Simplo GmbH v. Colibri Corp., 739 F. Supp. 2d 143, 147 (E.D.N.Y. 2010) (internal quotation marks and citations omitted).

ii. Facebook's Conduct as "Speaker or Publisher"

Plaintiffs next contend that the court "misapprehended" the scope of their claims in failing to consider Plaintiffs' allegation that Facebook "provided . . . terrorists with valuable services unrelated to publication . . . that do not fall within the traditional role of a publisher." (Recons. Mem. at 16.) In particular, Plaintiffs contend that they are suing Facebook for "developing, encouraging, and facilitating connections between terrorists," and not simply based on its failure to "police its accounts" and remove terrorist-affiliated users. (Id.)

In the court's view, however, it has already addressed Plaintiffs' argument and need not revisit its conclusions on that point. It is true that the court's previous opinion focused largely on whether Facebook's provision of accounts to Hamas-affiliated users could meaningfully be separated from its role as a "publisher or speaker" of content produced by users, with the court concluding that "Facebook's choices as to who may use its platform are inherently bound up in

its decisions as to what may be said on its platform, and so liability imposed based on its failure to remove users would equally "derive[] from [Facebook's] status or conduct as a 'publisher or speaker.'" (May 18 M&O at 21 (quoting LeadClick Media, 838 F.3d at 175).) While Plaintiffs now seek to distinguish between "making [Facebook's] system available to terrorists and a terrorist organization" and "provid[ing] [] terrorists with valuable services" through such access (Recons. Mem. at 16), this is a distinction without a difference: the "valuable services" at issue are part and parcel of access to a Facebook account, and so imposing liability on that basis would again effectively turn on "Facebook's choices as to who may use its platform." (May 18 M&O at 21.) Plaintiffs are merely attempting to rehash arguments that the court has already considered and rejected, which are insufficient to merit reconsideration.[2] See Shrader, 70 F.3d at 257 ("[A] motion to reconsider should not be granted where the moving party seeks solely to relitigate an issue already decided.").

*c. Interplay Between the CDA and the ATA*

Plaintiffs next argue that, even if Section 230 would otherwise apply to the challenged conduct, it cannot apply here because such application "would be in direct conflict with the ATA." (Recons. Mem. at 19.) Though presented in several ways, Plaintiffs' essential argument is two part: (1) the ATA's goal of imposing expansive civil liability for harms resulting from terrorism is at odds with immunity under Section 230; and (2) because the ATA was adopted and amended after the CDA, it supersedes Section 230. (Id. at 17-23.)

[2] Plaintiffs make the related argument that the court simply erred in its conclusion that Section 230 protects Facebook from liability based on its provision of user accounts and platform services to Hamas-affiliated users. (Recons. Mem. at 17-18.) However, Plaintiff provides no contrary controlling authority, but only argues the court unduly expanded the scope of Section 230's coverage beyond that envisioned by the Second Circuit. (Id. at 18.) As with Plaintiffs' more indirect attack on the court's holding discussed above, the court sees no reason to permit relitigation of issues already decided simply because Plaintiffs are dissatisfied with the court's prior decision.

At the outset, the court notes that it is skeptical that this argument is properly raised in the instant motion, as it can hardly be said to have been fully presented previously. Plaintiffs first advanced this argument in a single line in a footnote in their brief opposing Facebook's motion to dismiss. (See Pls. MTD Opp'n at 27 n.6 ("Even if there were a conflict between the limited immunity granted by the CDA and the liability imposed by the ATA, the ATA would control as its later enactment would be a tacit limiting of the CDA.").) Expanding this line to encompass five pages of their present briefing seems to the court to be the very definition of impermissibly "advanc[ing] . . . arguments not previously presented to the court." Schoolcraft, 248 F. Supp. 3d at 508 (internal quotation marks and citations omitted).

Even if Plaintiffs' argument is not waived, however, it is meritless. Quoting from the preamble to the most recent amendment to the ATA, Plaintiffs contend that immunizing Facebook under Section 230 frustrates Congress's purpose of "provid[ing] civil litigants with the broadest possible basis . . . to seek relief against entities . . . that have provided material support, whether directly or indirectly, to foreign organizations or persons that engage in terrorist activities."[3] (Recons. Mem. at 21 (quoting Justice Against Sponsors of Terrorism Act ("JASTA"), § 2(b), Pub. L. No. 114-222, 130 Stat. 852, 853).) Plaintiffs do not suggest that the ATA explicitly limits Section 230 immunity, however, but instead argue that the ATA's later-in-time enactment and the broad policy statements quoted above implicitly displace Section 230 with respect to ATA-based civil actions. (Id. at 21-23.)

"When it is claimed that a later enacted statute creates an irreconcilable conflict with an earlier statute, the question is whether the later statute, by implication, has repealed all or, more

[3] While it is not necessary to the decision here, the court notes that, whatever their interpretive value, statements of purpose contained in the preamble to a statute are not part of the substantive scope of the law itself. See, e.g., 73 Am. Jur. 2d Statutes § 101 (2d ed. updated Nov. 2017).

typically, part of the earlier statute." Garfield v. Ocwen Loans Servicing, LLC, 811 F.3d 86, 89 (2d Cir. 2016). "[R]epeals by implication are not favored." In re Stock Exch. Options Trading Antitrust Litig., 317 F.3d 134, 144 (2d Cir. 2003) (quoting United States v. Borden Co., 308 U.S. 188, 198 (1939)). Accordingly, courts must not "infer a statutory repeal unless the later statute expressly contradicts the original act or unless such construction is absolutely necessary in order that the words of the later statute shall have any meaning at all." Nat'l Ass'n of Home Builders v. Defenders of Wildlife, 551 U.S. 644, 662 (2007) (internal quotation marks and citations omitted, and alterations omitted); see also Radzanower v. Touche Ross & Co., 426 U.S. 148, 155 (1976) ("The statutory provisions at issue here cannot be said to be in 'irreconcilable conflict' in the sense that there is a positive repugnancy between them or that they cannot mutually co-exist."). "[A] statute dealing with a narrow, precise, and specific subject is not submerged by a later enacted statute covering a more generalized spectrum." Nat'l Ass'n of Home Builders, 551 U.S. at 663 (quoting Radzanower, 426 U.S. at 153).

The court sees no reason to conclude that the ATA impliedly abrogated Section 230, as each statute can be enforced without depriving the other of "any meaning at all." Id. at 662. The ATA's civil recovery provisions create a broad right of recovery for U.S. nationals injured by acts of international terrorism, without differentiating based on the particular defendants against whom claims are raised. 18 U.S.C. § 2333. In enacting Section 230, however, Congress "was focusing on the particularized problems of [providers and users of interactive computer services] that might be sued in the state or federal courts," Radzanower, 426 U.S. at 153, limiting the liability of a narrow subset of defendants for a particular type of claims. Thus, the ATA's general cause of action for victims of international terrorism cannot be said to "expressly contradict[]" the CDA, nor does the Section 230's limitation on certain theories of liability

deprive the ATA of "any meaning at all." Nat'l Ass'n of Home Builders, 551 U.S. at 662. Said differently, the two acts can be read without any conflict: Section 230 provides a limited defense to a specific subset of defendants against the liability imposed by the ATA.

In contrast to the direction provided by the Supreme Court and Second Circuit to act cautiously in inferring statutory repeal, Plaintiffs urge an approach that would treat any statute that imposes liability and which was enacted after the CDA as implicitly limiting the reach of Section 230 absent an affirmative contrary statement. This approach would effectively reverse the presumption against inferring repeal and is patently inconsistent with the law outlined above.[4]

Accordingly, the court sees no reason to conclude that the ATA implicitly limited or repealed Section 230 or any other part of the CDA or to reconsider its prior opinion on that basis.

*d. Application of the CDA to Plaintiffs' Israeli Law Claims*

Plaintiffs' final argument is that the court erred in applying Section 230 to Plaintiffs' Israeli-law claims. (Recons. Mem. at 24-25.) Plaintiffs argue that court should have conducted a conflict-of-laws analysis, which would have demonstrated that Israeli (as opposed to New York) law applied to a number of Plaintiffs' claims. (Id. at 24-25.) From this, Plaintiffs contend that the court should not have applied Section 230 to the Israeli law claims, as the CDA "is a feature of American law that has no corollary in Israel." (Id. at 25.)

Plaintiffs' argument misunderstands the court's prior opinion, which addressed the issue raised. Noting that Plaintiffs contended that Section 230 "does not apply to claims based in foreign law," the court assumed that the Plaintiffs' Israeli tort claims were properly presented

[4] Plaintiffs make the related argument that the court's interpretation of Section 230 "yields results that can only be described as 'absurd'" when applied to the ATA. (Recons. Mem. at 23-24.) This argument, which is unsupported by citation to legal authority, is not properly presented on a motion for reconsideration, and so the court does not address it.

and concluded those claims were barred in any event. (May 18 M&O at 27 n.14.) In coming to this determination, the court examined the enumerated exceptions to Section 230's grant of immunity, and concluded that the absence of any carve-out for claims based on foreign law indicated that no such exception was intended. (Id.)

To the extent that Plaintiffs argue that a conflict-of-laws analysis prevents the application of federal statutes to foreign-law-based claims, the argument is unsupported in law or logic. Plaintiffs point to no authority for the notion that the decisional rules applied in a conflict-of-laws analysis require courts in this country to ignore governing sources of federal law when applying claims raised under the laws of other nations,[5] nor is the court aware of any such authority. Further, Plaintiffs' suggestion appears to be fundamentally at odds with supremacy of federal law over state law. When conducting a conflict-of-laws analysis, federal courts look to the law of the forum state, in this case New York. Cf., e.g., Licci ex rel. Licci v. Lebanese Canadian Bank, SAL, 672 F.3d 155, 157 (2d Cir. 2012) ("A federal court sitting in diversity or adjudicating state law claims that are pendent to a federal claim must apply the choice of law rules of the forum state." (internal quotation marks and citation omitted)). It is almost too obvious to state that New York law, including the law governing conflict of laws, could not direct courts to disregard federal law. Cf. Figueroa v. Foster, 864 F.3d 222, 227 (2d Cir. 2017) ("Under the Supremacy Clause of the Constitution, state and local laws that conflict with federal law are without effect." (internal quotation marks and citation omitted)). Finally, the court notes

[5] Instead, Plaintiffs cite to cases considering conflicts of law between the laws of individual states and other states or foreign nations or between the laws of two foreign nations. See Licci ex rel. v. Lebanese Canadian Bank, SAL, 672 F.3d 155, 157-58 (2d Cir. 2012); Fin. One Pub. Co. Ltd. v. Lehman Bros. Special Fin., Inc., 414 F.3d 325, 331-339 (2d Cir. 2005) (same as to New York and Thai law); Cooney v. Osgood Mach., Inc., 81 N.Y.2d 66, 75 (N.Y. 1993) (same as to New York and Missouri law); Schultz v. Boy Scouts of Am., Inc., 65 N.Y.2d 189, 194-204 (N.Y. 1985) (same as to New York and New Jersey law); Wultz v. Islamic Rep. of Iran, 755 F. Supp. 2d 1, 78-80 (D.D.C. 2010) (same as to laws of China and Israel).

that the application of Section 230's affirmative defense to Israeli claims is sensible under the circumstances, as it avoids the perverse result that plaintiffs could bring claims in American courts under foreign law that would be barred if brought under federal or state law.

Accordingly, and again assuming that Israeli law, not New York law, applies to the cited claims, the court is not convinced that its prior decision was erroneous.

* * * *

For the foregoing reasons, Plaintiffs' motion to alter the judgment pursuant to Federal Rule of Civil Procedure 59(e) is DENIED.

**B. Motion to Amend the Complaint**

In the alternative, Plaintiffs move to amend their complaint a second time and propose new allegations which, in their account, correct the deficiencies in their prior complaint. (Amendment Mot.; Pls. Mem. in Supp. of Amendment Mot. ("Amendment Mem.") (Dkt. 53); see also PSAC.) After considering the proposed second amended complaint, the court concludes that Plaintiffs fail to allege facts that would support any of the asserted causes of action against Facebook. Their motion to amend is accordingly denied.

1. Legal Standard

Under Federal Rule of Civil Procedure 15(a), a party may amend its complaint either with its opponent's written consent or with leave of the court.[6] Fed. R. Civ. P. 15(a)(2). Courts "should freely give leave [to amend] when justice so requires." Id. Accordingly, requests to amend should be generally be granted absent a showing of "'undue delay, bad faith or dilatory motive on the part of the movant, repeated failure to cure deficiencies by amendments previously allowed, undue prejudice to the opposing party . . . [or] futility of amendment.'" Conforti v.

[6] Rule 15(a) also permits amendment once as a matter of course within set time periods. That provision is not relevant here, however, not least because Plaintiffs have already amended their complaint once before.

Sunbelt Rentals, Inc., 201 F. Supp. 3d 278, 290-91 (E.D.N.Y. 2016) (quoting Dougherty v. Town of N. Hempstead Bd. of Zoning Appeals, 282 F.3d 83, 87 (2d Cir. 2002)) (alterations in original). In considering whether an amendment would be "futile," courts apply the same standard of legal sufficiency as that employed in motions to dismiss, see Thea v. Kleinhandler, 807 F.3d 492, 496-97 (2d Cir. 2015), considering whether the proposed amended complaint "contain[s] sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face,'" Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007)).

Leave to amend may be granted post-judgment. "As a procedural matter, '[a] party seeking to file an amended complaint postjudgment must first have the judgment vacated or set aside pursuant to [Rules] 59(e) or 60(b).'" Williams v. Citigroup Inc., 659 F.3d 208, 213 (2d Cir. 2011) (quoting Ruotolo v. City of New York, 514 F.3d 184, 191 (2d Cir. 2008)). In such cases, however, "Rule 15's liberality must be tempered by considerations of finality." Id.

2. Application

In their proposed second amended complaint ("PSAC"), Plaintiffs propose to add a number of allegations that fall into four primary categories: (1) "[f]actual background and legislative statements involved in the enactment of the federal antiterrorism statutes at issue" (Amendment Mem. at 4); (2) allegations that Facebook violated the ATA by providing material support to Hamas in the form of "personnel" and "expert assistance" (id. at 3-4), and that Facebook's assistance to Hamas "freed-up money and other resources for Hamas and the terrorists to carry out the terrorist acts that severely injured the Plaintiffs" (id. at 7); (3) allegations related to Facebook users' ability to "self-publish" (id. at 4); and (4) Allegations demonstrating that Facebook's actions pertaining to its provision of material support and resources to Hamas occurred" outside of the United States (id. at 6). Additionally, Plaintiffs

propose adding a new claim under 18 U.S.C. § 2339C(c) based on Facebook's purported concealment of material resources provided to Hamas, as well as factual allegations related to that claim. The court examines each of these categories of proposed amendments and, for the reasons that follow, denies the motion to amend as futile.

*a. Allegations Regarding Antiterrorism Statutes*

The first category of new proposed new allegations pertains only to the background of the two antiterrorism statutes at issue here, the ATA and JASTA. (Id. at 4.) These allegations include a history of the ATA's enactment (PSAC ¶¶ 2-7, 18-53), including specifically the act's civil enforcement provisions (id. ¶¶ 38-44). Plaintiffs' evident purpose in introducing this background is to demonstrate that civil claims for material support fall outside of Section 230's grant of immunity based on an exception within that section, which states that "[n]othing in this section shall be construed to impair the enforcement of . . . any . . . Federal criminal statute." 47 U.S.C. § 230(e)(1). Plaintiffs contend that the background and legislative history of the ATA and JASTA show that the creation of civil remedies for violations of criminal statutes prohibiting terrorism were meant to facilitate "enforcement" of those statutes.[7] (Pls. Reply in Supp. of Amendment Mot. ("Amendment Reply") (Dkt. 59) at 2-3.)

Plaintiffs' arguments are unpersuasive. The court addressed Section 230's exception for enforcement of federal criminal laws in its previous opinion, noting that "most courts that have examined" that subsection have concluded that it does not "inhibit immunity as to civil liability

[7] Plaintiffs also argue that the text and legislative history of the ATA and, particularly, JASTA, demonstrate that "Congress deems ATA claims supremely important, and insofar as other statute or regulations—including the CDA—are inconsistent with this most recent expression of Congress's intent, the ATA claims must prevail." (Pls. Reply in Supp. of Amendment Mot. ("Amendment Reply") (Dkt. 59) at 4-6.) This argument effectively retreads Plaintiffs' contention that the ATA and JASTA implicitly repeal the CDA to the extent of any conflict. For the same reasons that it denied the motion for reconsideration, the court concludes that Plaintiffs' proposed amendments on this point are futile.

predicated on federal criminal statutes." (May 18 M&O at 21 n.11.) In this regard, the court finds particularly convincing the First Circuit's conclusion that Section 230(e)(1)'s specific reference to "criminal statutes," viewed alongside other exceptions within Section 230 that apply equally to civil and criminal remedies, indicates that Congress only intended to exclude criminal prosecutions through that exception.[8] Jane Doe No. 1 v. Backpage.com, 817 F.3d 12, 23 (1st Cir. 2016). The court agrees with this reasoning and concludes that the "enforcement"[9] of "Federal criminal statutes" in this context was intended only to extend to enforcement by means of a criminal proceeding.

Accordingly, the court finds these new allegations regarding the history and purpose of the ATA and JASTA to be insufficient to overcome previously identified shortcomings in Plaintiffs' first amended complaint.

*b. Additional Material Support Allegations and Self-Publication*

Plaintiffs' proposed complaint also attempts to refine its allegations that Facebook provided material support to terrorism so as to avoid involving implicating Facebook's role as a

[8] Plaintiffs attempt to distinguish Jane Doe and other cases cited in the court's previous opinion on the basis that the statutes cited therein "permitted recovery of compensatory damages, not punitive or exemplary damages [as] permitted by the ATA." (Amendment Reply at 3 (emphasis in original).) However, the First Circuit reasoned in Jane Doe from the language of the statute itself that Section 230(e)(1) excepts only criminal actions to enforce criminal statutes, 817 F.3d at 23, which means that the purposes of a particular civil action are irrelevant. Further, the court notes that Plaintiffs appear to be incorrect in their contention that the statute at issue in Jane Doe does not permit punitive damages in civil suits. While the statute and Second Circuit case law do not provide direct guidance on the point, the Ninth Circuit concluded that the civil remedies available under that section include punitive damages. See Ditullio v. Boehm, 662 F.3d 1091, 1098 (9th Cir. 2011); see also Walia v. Veritas Healthcare Solutions, L.L.C., No. 13-CV-6935 (KPF), 2015 WL 4743542, at *10 n.15 (S.D.N.Y Aug. 11, 2015).

[9] Plaintiffs point to a statement by the Second Circuit that "the ATA's legislative history reflects that Congress conceived of the ATA, at least in part, as a mechanism for protecting the public's interests through private enforcement." Linde v. Arab Bank, PLC, 706 F.3d 92, 112 (2d Cir. 2013). The court is not convinced that this language, which appears in dicta and arose in the entirely different context of international comity analysis, implies that private suits to enforce the ATA are, in effect, on the same footing as are prosecutions under that law. Moreover, as stressed above, the task before the court is not to interpret the ATA, but to determine the meaning of Section 230(e)(1). As the court has already determined that Section 230's reference to "enforcement . . . of any . . . Federal criminal statutes" is specific to criminal prosecutions, it need not ascertain whether civil provisions of other statutes were envisioned as providing a secondary means of enforcement.

publisher or speaker of third-party content. First, Plaintiffs attempt to differentiate Facebook from other websites by stressing that Facebook users register to "design and create their own internet website," from which they are free to "self-publish" content without Facebook purporting to act as "editor, publisher, or speaker" of its users' postings. (PSAC ¶ 127-28.) Second, Plaintiffs add new allegations regarding the types of "material support" that Facebook provides. They characterize Facebook as providing "personnel" to Hamas by "making Hamas leaders, operatives, and recruits available to Hamas to conspire, plan, prepare, and carry out terrorist activity." (PSAC ¶ 223.) Plaintiffs also contend that Facebook provides "expert services" to Hamas-affiliated users by allowing them access to its platform and, through such access, "highly advanced software, algorithms, computer servers and storage, communications devices, [and] computer applications" that Facebook provides to all users. (Id. ¶¶ 123-24; see also Amendment Mem. at 5.)

Plaintiffs' additional allegations do nothing to address the shortcomings in their theories of liability identified in the court's previous decision. With respect to the allegations regarding "self-publication," Plaintiffs misinterpret the scope of Section 230's immunity. Plaintiffs repeatedly stress that users' introduction of information onto Facebook's eponymous platform occurs without Facebook "exercis[ing] any editorial discretion when providing registered accounts or over what users publish on their own [] accounts." (Amendment Reply at 8.) From this, Plaintiffs appear to suggest that Facebook cannot be exercising any editorial or publication functions protected by Section 230 which, they imply, require some specific selection with respect to the particular users or postings that may appear on its platform. This argument misunderstands the court's prior decision: In the court's view, Facebook's decision to keep its platform as an open forum, available for registration and posting without prior approval from

Facebook, is itself an exercise of editorial discretion. (May 18 M&O at 21.) As noted by the First Circuit:

> [the plaintiffs-appellants'] well-pleaded claims address the structure and operation of the [defendant-appellee's] website, that is, [defendant's] decisions about how to treat postings. Those claims challenge features that are part and parcel of the overall design and operation of the website (such as the lack of phone number verification, the rules about whether a person may post after attempting to enter a forbidden term, and the procedure for uploading photographs). Features such as these, which reflect choices about what content can appear on the website and in what form, are editorial choices that fall within the purview of traditional publisher functions.

Jane Doe, 817 F.3d at 21. The same reasoning supports both the court's previous decision and its conclusion here that allegations regarding "self-publication" do not exempt Plaintiffs' claims from Section 230's coverage: Facebook's decisions regarding the "overall design and operation of its website," including the criteria (or lack thereof) for obtaining an account and posting on the platform are themselves "editorial choices that fall within the purview of traditional publisher functions." Id.; see also Fields v. Twitter, Inc., 217 F. Supp. 3d 1116, 1124 (N.D. Cal. 2016) (holding that the defendant's "decisions to structure and operate itself as a 'platform . . . allow[ing] for the freedom of expression of hundreds [of] millions of people around the world,' and, through its hands-off policy, allowing [a terrorist group] to obtain 'dozens of accounts on its social network' 'reflect choices about what [third-party] content can appear on [Twitter] and in what form.'" (internal quotation marks and citations omitted; alterations in original)). Plaintiffs' new allegations that these policies allow users to join Facebook's platform and to "self-publish" without Facebook's prior approval do not alter the conclusion that Facebook's decisions regarding the structure of its platform fall within the traditional functions of a publisher and so that Plaintiffs' theory relies only on a "duty . . . derive[d] from [Facebook's] status or conduct as a 'publisher or speaker.'" LeadClick Media, 838 F.3d at 175.

Plaintiffs' new allegations regarding Facebook's alleged provision of "personnel" and "expert services" to Hamas and Hamas-affiliated users suffer from the same flaw. Plaintiffs claim that "technological tools" Facebook provided to its users, and that these tools are unrelated to the content of the underlying communications. (Amendment Reply at 8; see also Amendment Mem. at 4-5.) Plaintiffs contend these tools provided to users "extend[] far beyond providing or performing traditional services of a publisher," and so are not within the scope of the services of a 'publisher.'" (Amendment Reply at 7-8.) At root, however, these theories again derive from a claimed duty on Facebook's part to prevent certain users from using its platform and seek to impose liability based on Facebook's decision to allow free access to, and use of, its platform and forum. Said differently, Facebook is alleged to have violated a duty to prevent certain users from accessing and using its platform. As discussed above and in this court's previous dismissal of Plaintiffs' claims, Section 230 shields Facebook from such claims, as "Facebook's choices as to who may use its platform are inherently bound up in its decisions as to what may be said on its platform, and so liability imposed based on its failure to remove users would equally 'derive[] from [Facebook's] status or conduct as a 'publisher or speaker.'"" (May 18 M&O at 21 (quoting LeadClick Media, 838 F.3d at 175).)

Moreover, like Plaintiffs' first amended complaint, Plaintiffs' new allegations regarding Facebook's claimed provision of "personnel" and "expert services" again "rely on content to establish causation and, by extension, Facebook's liability," a theory already rejected by this court. (May 18 M&O at 22.) As Plaintiffs' proposed amended complaint makes clear, their theory that Facebook makes "personnel" available to Hamas depends on the content of communications on Facebook's website: Plaintiffs seek to hold Facebook liable for providing a publication forum for Hamas and its leaders, operatives, and recruits, "to conspire, plan, prepare,

and carry out terrorist activity." (SAC ¶ 223.) This is fundamentally no different than Plaintiffs' prior argument that "Facebook contributed to their harm by allowing Hamas to use its platform to post particular offensive content." (May 18 M&O at 22.) Likewise, both the "personnel" and "expert services" allegations appear to rest in large part on allegations that Facebook's networking algorithms recommend content to account holders. However, as Facebook points out, "the features of Facebook that [P]laintiffs criticize operate solely in conjunction with . . . content posted by Facebook users." (See Def. Opp'n to Amendment Mot. ("Amendment Opp'n") (Dkt. 57) at 5 (emphasis in original); see also PSAC ¶¶ 611-22 (describing how Facebook's algorithms connect "users to one another and to groups and events that they will be interested in based on the information in their user profiles and online activities"). Plaintiffs' new allegations would again simply seek to hold Facebook liable solely on the basis of the website's role in hosting and re-publishing content generated by Hamas-affiliated users.[10] Bound up as they are in the content that Hamas-affiliated users provide, the court concludes that these new claims remain subject to the immunity afforded under Section 230 and so cannot provide a basis for liability as to Facebook.[11]

---

[10] Plaintiff also proposes to add new allegations regarding additional "predicate" acts of terrorism by Hamas. (PSAC ¶¶ 648-49; Amendment Mem. at 7.) Plaintiffs contend that these additional predicate acts support the conclusion that "Facebook's liability does not depend upon attributing the content of Hamas' Facebook posts to Facebook." (Amendment Mem. at 7.) In particular, Plaintiffs point to the "aiding and abetting" charges brought under JASTA and argue that "once Facebook . . . provid[es] material support to Hamas, Facebook is liable under [JASTA] for any reasonably foreseeable injury that may result from Hamas's use of that material support." (Amendment Reply at 9.) These proposed amendments do nothing to address or sidestep the basis for the court's prior dismissal of Plaintiffs' claims: regardless of the predicate acts at issue, the only basis that Plaintiffs propose for imposing liability on Facebook for "aiding and abetting" or providing "material support" to those terroristic crimes is Facebook's decision to permit Hamas-affiliated users to use its platform. The court has repeatedly rejected that theory, and so the proposed amendments do not further Plaintiffs' entitlement to relief.

[11] Plaintiffs also propose alleging that, because of its use of Facebook, Hamas was able to "allocate other financial resources to terrorist activities." (Amendment Reply at 10; see also PSAC ¶ 219.) Plaintiffs are correct that this allegation could support a claim under the material support statutes. See, e.g., Holder v. Humanitarian Law Project, 561 U.S. 1, 30 (2010). In light of the court's conclusion that the Plaintiffs' material support claims are not viable because they rely on theories barred by Section 230, however, these allegations do not support Facebook's liability.

*c. Extraterritoriality Allegations*

Plaintiffs' proposed amendments include a number of factual allegations regarding Facebook's conduct outside of the United States, which Plaintiffs contend "support [their] contention that the CDA does not apply to claims involving violation of laws outside of the territorial jurisdiction of the United States." (Amendment Reply at 10; PSAC ¶¶ 629-32.) The court need not dwell on these new allegations. The court concluded in its prior opinion that, for purposes of the extraterritoriality analysis, the relevant territorial relationships are based "where redress is sought and immunity is needed"—the situs of the litigation. (May 18 M&O at 27.) Plaintiffs' new allegations obviously do not suggest that the situs of this litigation has changed, but are better viewed as part of their tenacious effort to convince the court to reconsider its prior extraterritoriality analysis. The court has already declined to do so, and so concludes that these new allegations fail to advance Plaintiffs' claims.

*d. "Concealment" of Material Support*

Plaintiffs' final set of new allegations relates to their new claim that Facebook "concealed" its provision of material support to Hamas in violation of the ATA. Specifically, Plaintiffs allege that Facebook's "Community Standards," which purport to prevent terrorists and terrorist organizations to use the platform, "conceal" both Facebook's own provision of material support to Hamas and the separate use of the platform by terrorists to provide material support to Hamas. (Amendment Mem. at 6.)

The relevant section of the material support statutes prohibits covered individuals and entities[12] from "knowingly conceal[ing] or disguis[ing] the nature, location, source, ownership,

[12] Specifically, the prohibition applies to individuals and entities in the United States or outside of the United States if they are either "a national of the United States or a legal entity organized under the laws of the United States (including any of its States, districts, commonwealths, territories, or possession)[.]" 18 U.S.C. § 2339C(c)(1)(A)-(B). Facebook does not argue that it falls outside this coverage.

or control of any material support or resources, or any proceeds of such funds . . . knowing or intending that the support or resources are to be provided, or . . . were provided, in violation of section 2339B[.]" 18 U.S.C. § 2339C(c)(2)(A). Thus, in order to violate that provision, the entity must have knowingly "concealed" or "disguised" material support provided to a designated foreign terrorist organization[13] but need not necessarily have provided the material support itself.

In the court's view, allegations brought under that section against Facebook, if plausibly pled, would escape Section 230's coverage. In its opposition to the amendment, Facebook argues strenuously that the "concealment claim boils down to a challenge to who may use Facebook and what content they share" and so seeks to impose liability on the same basis already rejected by the court. (Def. Suppl. Opp'n to Amendment Mot. (Dkt. 60) at 3.) It may be true that a concealment claim based only on Facebook's own purported provision of material support would fail: As noted, Section 2339C(c) requires a predicate violation of Section 2339B, 18 U.S.C. § 2339C(c)(2)(A), and the court has already held that Facebook cannot be held liable under that statute based on Plaintiffs' theories. Plaintiffs also contend, however, that Facebook's statements in the Community Standards "conceal" acts by Hamas members and supporters that provide material support to Hamas using Facebook's platform. (Amendment Mem.. at 6 ("By its actions and deceptions, Facebook also conceals the Hamas leaders' and affiliates' own provision of personnel (themselves) via their Facebook accounts." (emphasis in original)); PSAC ¶¶ 222-24.) Said differently, unlike the other theories of liability proposed by Plaintiffs, the "concealment" claim does not seek to hold Facebook liable for failing to prevent Hamas and its

[13] 18 U.S.C. § 2339B applies only to material support provided to designated foreign terrorist organizations. 18 U.S.C. § 2339B(a).

affiliates from obtaining accounts or posting offensive content. (See May 18 M&O, at 21-22.) Instead, Plaintiffs argue that Facebook's own actions conceal or disguise material support to Hamas provided by others. The court agrees that, thus construed, the concealment cause of action does not fall within the coverage of Section 230, as it does not "inherently require[] the court to treat [Facebook] as the publisher or speaker of content provided by another," or "derive[] from [Facebook's] status or conduct as a 'publisher or speaker.'" (Id. at 20 (quoting LeadClick Media, 838 F.3d at 175).

This does not end the inquiry, however, as Plaintiffs must still set forth sufficient allegations "to state a claim to relief that is plausible on its face." Iqbal, 556 U.S. at 678 (internal quotation marks and citation omitted). The key question in this instance is whether the proposed amendments set forth a sufficient factual basis for the court to conclude that Facebook "concealed" or "disguised" material support to Hamas provided using its platform. The statute does not define those terms, nor does any court appear to have interpreted them in the context of this or similar statutes.[14] "[W]here a statute does not define a term, we give the term its ordinary meaning." EMI Christian Music Grp., Inc. v. MP3Tunes, LLC, 844 F.3d 79, 89 (2d Cir. 2016) (internal quotation marks and citation omitted). The Merriam-Webster dictionary defines "conceal" as, inter alia, "to prevent disclosure or recognition of," Conceal, Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/conceal (last visited Jan. 8, 2018), and "disguise" as, inter alia, "to obscure the existence or true state or character of," Disguise, Merriam-Webster Online Dictionary, https://www.merriam-

[14] Similar language appears in 18 U.S.C. § 2339A (criminalizing "conceal[ing] or disguise[ing] the nature, location, source, or ownership of material support or resources") and various places in 18 U.S.C § 1956 (defining money laundering transaction to include transactions intended "to conceal or disguise the nature, location, source, ownership, or control of property believed to be the proceeds of specified unlawful activity"). The court reviewed cases interpreting the terms "conceal" and "disguise" in the context of those statutes as well, but found no helpful guidance.

webster.com/dictionary/disguise (last visited Jan. 8, 2018). Thus, in order to avoid the conclusion that leave to amend should be denied as futile, Plaintiffs must present facts sufficient to show that Facebook's actions either prevented "disclosure or recognition" of Hamas' use of its platform or "obscured the existence or true state or character" of that use.

After examining the allegations set forth in the proposed amended complaint, the court concludes that Plaintiffs fail to set forth a plausible claim that Facebook "concealed" or "disguised" the use of its platform by Hamas and its member and supporters. As noted, Plaintiffs' claims that Facebook conceals Hamas's presence on its platform are based solely on allegedly false claims in Facebook's "Community Standards" and public statements by the company that it does not permit terrorists or terrorist organizations to use the website. (See Pls. Suppl. Mem. in Supp. of Amendment Mot. (Dkt. 61) at 5-6; see also, e.g., PSAC ¶¶ 172-74, 583-89.) Plaintiffs do not allege, however, that such false statements had the effect of preventing anyone from discovering that Hamas or its members were using Facebook's platform. At most, the policy statements and public pronouncements to which Plaintiffs point have the effect of concealing or disguising Facebook's factual willingness to abide such use, but not the fact of the use itself. To the contrary, the complaint is replete with allegations that "HAMAS, its leaders, spokesmen, and members have openly maintained and used official Facebook accounts" (PSAC ¶ 9), use those accounts to draw attention to their activities (PSAC ¶ 165), and that this use of the platform by Hamas and other, similar groups has been widely recognized by the public (id. ¶¶ 590-98). Against these allegations, the court sees no plausible claim that Facebook's statements—or any other action by the company, for that matter—did anything to "prevent

disclosure or recognition" or "obscure the existence or true . . . character of" the use of its platform to support Hamas.[15]

* * * *

Accordingly, Plaintiffs' motion to amend their complaint is pursuant to Federal Rules of Civil Procedure 15(a), 59(e), and 60(b) is denied. Moreover, as the proposed amendments fail to correct the deficiencies identified by the court's decision dismissing Plaintiffs' first amended complaint, the court concludes that it is appropriate to deny the motion with prejudice. See, e.g., Curtis v. Citibank, N.A., 204 F. App'x 929, 932 (2d Cir. 2006) (summary order) (holding that dismissal with prejudice was within the court's discretion where plaintiff had notice of and failed to correct deficiencies in complaint).

## III. CONCLUSION

For the foregoing reasons, Plaintiffs' motions to amend the judgment (Dkt. 50) and to file a second amended complaint (Dkt. 52) are DENIED WITH PREJUDICE.

SO ORDERED.

s/Nicholas G. Garaufis
NICHOLAS G. GARAUFIS
United States District Judge

Dated: Brooklyn, New York
January 17, 2018

[15] In their supplemental brief in support of the concealment claim, Plaintiffs also request leave to amend their complaint—again—to include allegations related to testimony by Facebook's general counsel before the United States Senate. (Pls. Suppl. Mem. in Supp. of Amendment Mot. at 9-10.) Plaintiffs do not, however, state how this information would support any of their claims, leaving the court without any basis to assess the utility or futility of such amendments. Particularly in light of court's existing judgment against Plaintiff, the court finds that considerations of finality outweigh any interest in allowing Plaintiffs to submit another round of amendments and denies the motion accordingly. Cf. Williams, 659 F.3d at 213 ("Where . . . a `party does not seek leave to file an amended complaint until after judgment is entered, Rule 15's liberality must be tempered by considerations of finality.").

**18 U.S.C. 2331 – Definitions**

As used in this chapter—

**(1)** the term "international terrorism" means activities that—

**(A)** involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State;

**(B)** appear to be intended—

**(i)** to intimidate or coerce a civilian population;
**(ii)** to influence the policy of a government by intimidation or coercion; or
**(iii)** to affect the conduct of a government by mass destruction, assassination, or kidnapping; and

**(C)** occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum;

**18 U.S.C. 2333 – Civil Remedies**

**(a) Action and Jurisdiction**— Any national of the United States injured in his or her person, property, or business by reason of an act of international terrorism, or his or her estate, survivors, or heirs, may sue therefor in any appropriate district court of the United States and shall recover threefold the damages he or she sustains and the cost of the suit, including attorney's fees. * * *

**(d) Liability**—

**(1) Definition**— In this subsection, the term "person" has the meaning given the term in section 1 of title 1.

**(2) Liability**— In an action under subsection (a) for an injury arising from an act of international terrorism committed, planned, or authorized by an organization that had been designated as a foreign terrorist organization under section 219 of the Immigration and Nationality Act (8 U.S.C. 1189), as of the date on which such act of international terrorism was committed, planned, or

authorized, liability may be asserted as to any person who aids and abets, by knowingly providing substantial assistance, or who conspires with the person who committed such an act of international terrorism.

**18 U.S.C. 2339A – Providing Material Support to Terrorists**

**(a) Offense**— Whoever provides material support or resources or conceals or disguises the nature, location, source, or ownership of material support or resources, knowing or intending that they are to be used in preparation for, or in carrying out, a violation of section 32, 37, 81, 175, 229, 351, 831, 842(m) or (n), 844(f) or (i), 930(c), 956, 1091, 1114, 1116, 1203, 1361, 1362, 1363, 1366, 1751, 1992, 2155, 2156, 2280, 2281, 2332, 2332a, 2332b, 2332f, 2340A, or 2442 of this title, section 236 of the Atomic Energy Act of 1954 (42 U.S.C. 2284), section 46502 or 60123(b) of title 49, or any offense listed in section 2332b(g)(5)(B) (except for sections 2339A and 2339B) or in preparation for, or in carrying out, the concealment of an escape from the commission of any such violation, or attempts or conspires to do such an act, shall be fined under this title, imprisoned not more than 15 years, or both, and, if the death of any person results, shall be imprisoned for any term of years or for life. A violation of this section may be prosecuted in any Federal judicial district in which the underlying offense was committed, or in any other Federal judicial district as provided by law.

**(b) Definitions**— As used in this section—

**(1)** the term "material support or resources" means any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials;

**(2)** the term "training" means instruction or teaching designed to impart a specific skill, as opposed to general knowledge; and

**(3)** the term "expert advice or assistance" means advice or assistance derived from scientific, technical or other specialized knowledge.

**18 U.S.C. 2339B – Providing Material Support or Resources to Designated Foreign Terrorist Organizations**

**(a) Prohibited Activities**—

**(1) Unlawful conduct**— Whoever knowingly provides material support or resources to a foreign terrorist organization, or attempts or conspires to do so, shall be fined under this title or imprisoned not more than 15 years, or both, and, if the death of any person results, shall be imprisoned for any term of years or for life. To violate this paragraph, a person must have knowledge that the organization is a designated terrorist organization (as defined in subsection (g)(6)), that the organization has engaged or engages in terrorist activity (as defined in section 212(a)(3)(B) of the Immigration and Nationality Act), or that the organization has engaged or engages in terrorism (as defined in section 140(d)(2) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989). * * *

**(d) Extraterritorial Jurisdiction**—

**(1) In general**— There is jurisdiction over an offense under subsection (a) if—

**(A)** an offender is a national of the United States...or an alien lawfully admitted for permanent residence in the United States...;
**(B)** an offender is a stateless person whose habitual residence is in the United States;
**(C)** after the conduct required for the offense occurs an offender is brought into or found in the United States, even if the conduct required for the offense occurs outside the United States;
**(D)** the offense occurs in whole or in part within the United States;
**(E)** the offense occurs in or affects interstate or foreign commerce; or
**(F)** an offender aids or abets any person over whom jurisdiction exists under this paragraph in committing an offense under subsection (a) or conspires with any person over whom jurisdiction exists under this paragraph to commit an offense under subsection (a).

**(2) Extraterritorial jurisdiction**— There is extraterritorial Federal jurisdiction over an offense under this section.

**18 U.S.C. 2339C – Prohibitions Against the Financing of Terrorism**

**(a) Offenses**—

**(1) In general**— Whoever, in a circumstance described in subsection (b), by any means, directly or indirectly, unlawfully and willfully provides or collects funds with the intention that such funds be used, or with the knowledge that such funds are to be used, in full or in part, in order to carry out—

**(A)** an act which constitutes an offense within the scope of a treaty specified in subsection (e)(7), as implemented by the United States, or

**(B)** any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act,

shall be punished as prescribed in subsection (d)(1).

**(2) Attempts and conspiracies**— Whoever attempts or conspires to commit an offense under paragraph (1) shall be punished as prescribed in subsection (d)(1).

**(3) Relationship to predicate act**— For an act to constitute an offense set forth in this subsection, it shall not be necessary that the funds were actually used to carry out a predicate act.

**(b) Jurisdiction**— There is jurisdiction over the offenses in subsection (a) in the following circumstances—

**(1)** the offense takes place in the United States and—

**(A)** a perpetrator was a national of another state or a stateless person;

**(B)** on board a vessel flying the flag of another state or an aircraft which is registered under the laws of another state at the time the offense is committed;

**(C)** on board an aircraft which is operated by the government of another state;

**(D)** a perpetrator is found outside the United States;

**(E)** was directed toward or resulted in the carrying out of a predicate act against—

**(i)** a national of another state; or
**(ii)** another state or a government facility of such state, including its embassy or other diplomatic or consular premises of that state;

**(F)** was directed toward or resulted in the carrying out of a predicate act committed in an attempt to compel another state or international organization to do or abstain from doing any act; or

**(G)** was directed toward or resulted in the carrying out of a predicate act—

**(i)** outside the United States; or
**(ii)** within the United States, and either the offense or the predicate act was conducted in, or the results thereof affected, interstate or foreign commerce;

**(2)** the offense takes place outside the United States and—

**(A)** a perpetrator is a national of the United States or is a stateless person whose habitual residence is in the United States;

**(B)** a perpetrator is found in the United States; or

**(C)** was directed toward or resulted in the carrying out of a predicate act against—

**(i)** any property that is owned, leased, or used by the United States or by any department or agency of the United States, including an embassy or other diplomatic or consular premises of the United States;
**(ii)** any person or property within the United States;
**(iii)** any national of the United States or the property of such national; or
**(iv)** any property of any legal entity organized under the laws of the United States, including any of its States, districts, commonwealths, territories, or possessions; * * *

**(e) Definitions**— In this section—

**(1)** the term "funds" means assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including coin, currency, bank credits, travelers checks, bank checks, money orders, shares, securities, bonds, drafts, and letters of credit; * * *

**(3)** the term "proceeds" means any funds derived from or obtained, directly or indirectly, through the commission of an offense set forth in subsection (a);

**(4)** the term "provides" includes giving, donating, and transmitting;

**(5)** the term "collects" includes raising and receiving;

**(6)** the term "predicate act" means any act referred to in subparagraph (A) or (B) of subsection (a)(1) * * *

## 47 U.S.C. 230 – Protection for Private Blocking and Screening of Offensive Material

**(a) Findings**— The Congress finds the following:

**(1)** The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.

**(2)** These services offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops.

**(3)** The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.

**(4)** The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.

**(5)** Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.

**(b) Policy**— It is the policy of the United States—

**(1)** to promote the continued development of the Internet and other interactive computer services and other interactive media;

**(2)** to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;

**(3)** to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;

**(4)** to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and

**(5)** to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

**(c) Protection for "Good Samaritan" blocking and screening of offensive material**

**(1) Treatment of publisher or speaker**— No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

**(2) Civil liability**— No provider or user of an interactive computer service shall be held liable on account of—

**(A)** any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

**(B)** any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).[1]

**(d) Obligations of interactive computer service**— A provider of interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections.

**(e) Effect on other laws**

**(1) No effect on criminal law**— Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, or any other Federal criminal statute.

---

[1] So in original. Probably should be "subparagraph (A)."

**(2) No effect on intellectual property law**— Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.

**(3) State law**— Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.

**(4) No effect on communications privacy law**— Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986 or any of the amendments made by such Act, or any similar State law.

**(f) Definitions**— As used in this section:

**(1) Internet**— The term "Internet" means the international computer network of both Federal and non-Federal interoperable packet switched data networks.

**(2) Interactive computer service**— The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

**(3) Information content provider**— The term "information content provider" means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.

**(4) Access software provider**— The term "access software provider" means a provider of software (including client or server software), or enabling tools that do any one or more of the following:

**(A)** filter, screen, allow, or disallow content;
**(B)** pick, choose, analyze, or digest content; or
**(C)** transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.

# TITLE V—OBSCENITY AND VIOLENCE

Communications Decency Act of 1996.
Law enforcement and crime.
Penalties.

## Subtitle A—Obscene, Harassing, and Wrongful Utilization of Telecommunications Facilities

**SEC. 501. SHORT TITLE.**

47 USC 609 note.

This title may be cited as the "Communications Decency Act of 1996".

**SEC. 502. OBSCENE OR HARASSING USE OF TELECOMMUNICATIONS FACILITIES UNDER THE COMMUNICATIONS ACT OF 1934.**

Section 223 (47 U.S.C. 223) is amended—

(1) by striking subsection (a) and inserting in lieu thereof:

"(a) Whoever—

"(1) in interstate or foreign communications—

"(A) by means of a telecommunications device knowingly—

"(i) makes, creates, or solicits, and

"(ii) initiates the transmission of,

any comment, request, suggestion, proposal, image, or other communication which is obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten, or harass another person;

"(B) by means of a telecommunications device knowingly—

"(i) makes, creates, or solicits, and

"(ii) initiates the transmission of,

any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication;

"(C) makes a telephone call or utilizes a telecommunications device, whether or not conversation or communication ensues, without disclosing his identity and with intent to annoy, abuse, threaten, or harass any person at the called number or who receives the communications;

"(D) makes or causes the telephone of another repeatedly or continuously to ring, with intent to harass any person at the called number; or

"(E) makes repeated telephone calls or repeatedly initiates communication with a telecommunications device, during which conversation or communication ensues, solely to harass any person at the called number or who receives the communication; or

"(2) knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity,

shall be fined under title 18, United States Code, or imprisoned not more than two years, or both."; and

(2) by adding at the end the following new subsections:

"(d) Whoever—

"(1) in interstate or foreign communications knowingly—

"(A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or

"(B) uses any interactive computer service to display in a manner available to a person under 18 years of age, any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication; or

"(2) knowingly permits any telecommunications facility under such person's control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity,

shall be fined under title 18, United States Code, or imprisoned not more than two years, or both.

"(e) In addition to any other defenses available by law:

"(1) No person shall be held to have violated subsection (a) or (d) solely for providing access or connection to or from a facility, system, or network not under that person's control, including transmission, downloading, intermediate storage, access software, or other related capabilities that are incidental to providing such access or connection that does not include the creation of the content of the communication.

"(2) The defenses provided by paragraph (1) of this subsection shall not be applicable to a person who is a conspirator with an entity actively involved in the creation or knowing distribution of communications that violate this section, or who knowingly advertises the availability of such communications.

"(3) The defenses provided in paragraph (1) of this subsection shall not be applicable to a person who provides access or connection to a facility, system, or network engaged in the violation of this section that is owned or controlled by such person.

"(4) No employer shall be held liable under this section for the actions of an employee or agent unless the employee's or agent's conduct is within the scope of his or her employment or agency and the employer (A) having knowledge of such conduct, authorizes or ratifies such conduct, or (B) recklessly disregards such conduct.

"(5) It is a defense to a prosecution under subsection (a)(1)(B) or (d), or under subsection (a)(2) with respect to the use of a facility for an activity under subsection (a)(1)(B) that a person—

"(A) has taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication specified in such subsections, which may involve any appropriate measures to restrict minors from such communications, including any method which is feasible under available technology; or

"(B) has restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number.

"(6) The Commission may describe measures which are reasonable, effective, and appropriate to restrict access to prohibited communications under subsection (d). Nothing in

this section authorizes the Commission to enforce, or is intended to provide the Commission with the authority to approve, sanction, or permit, the use of such measures. The Commission shall have no enforcement authority over the failure to utilize such measures. The Commission shall not endorse specific products relating to such measures. The use of such measures shall be admitted as evidence of good faith efforts for purposes of paragraph (5) in any action arising under subsection (d). Nothing in this section shall be construed to treat interactive computer services as common carriers or telecommunications carriers.

"(f)(1) No cause of action may be brought in any court or administrative agency against any person on account of any activity that is not in violation of any law punishable by criminal or civil penalty, and that the person has taken in good faith to implement a defense authorized under this section or otherwise to restrict or prevent the transmission of, or access to, a communication specified in this section.

"(2) No State or local government may impose any liability for commercial activities or actions by commercial entities, nonprofit libraries, or institutions of higher education in connection with an activity or action described in subsection (a)(2) or (d) that is inconsistent with the treatment of those activities or actions under this section: *Provided, however*, That nothing herein shall preclude any State or local government from enacting and enforcing complementary oversight, liability, and regulatory systems, procedures, and requirements, so long as such systems, procedures, and requirements govern only intrastate services and do not result in the imposition of inconsistent rights, duties or obligations on the provision of interstate services. Nothing in this subsection shall preclude any State or local government from governing conduct not covered by this section.

"(g) Nothing in subsection (a), (d), (e), or (f) or in the defenses to prosecution under subsection (a) or (d) shall be construed to affect or limit the application or enforcement of any other Federal law.

"(h) For purposes of this section—

"(1) The use of the term 'telecommunications device' in this section—

"(A) shall not impose new obligations on broadcasting station licensees and cable operators covered by obscenity and indecency provisions elsewhere in this Act; and

"(B) does not include an interactive computer service.

"(2) The term 'interactive computer service' has the meaning provided in section 230(e)(2).

"(3) The term 'access software' means software (including client or server software) or enabling tools that do not create or provide the content of the communication but that allow a user to do any one or more of the following:

"(A) filter, screen, allow, or disallow content;

"(B) pick, choose, analyze, or digest content; or

"(C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.

"(4) The term 'institution of higher education' has the meaning provided in section 1201 of the Higher Education Act of 1965 (20 U.S.C. 1141).

"(5) The term 'library' means a library eligible for participation in State-based plans for funds under title III of the Library Services and Construction Act (20 U.S.C. 355e et seq.).".

**SEC. 503. OBSCENE PROGRAMMING ON CABLE TELEVISION.**

Section 639 (47 U.S.C. 559) is amended by striking "not more than $10,000" and inserting "under title 18, United States Code,".

**SEC. 504. SCRAMBLING OF CABLE CHANNELS FOR NONSUBSCRIBERS.**

Part IV of title VI (47 U.S.C. 551 et seq.) is amended by adding at the end the following:

47 USC 560.

**"SEC. 640. SCRAMBLING OF CABLE CHANNELS FOR NONSUBSCRIBERS.**

"(a) SUBSCRIBER REQUEST.—Upon request by a cable service subscriber, a cable operator shall, without charge, fully scramble or otherwise fully block the audio and video programming of each channel carrying such programming so that one not a subscriber does not receive it.

"(b) DEFINITION.—As used in this section, the term 'scramble' means to rearrange the content of the signal of the programming so that the programming cannot be viewed or heard in an understandable manner.".

**SEC. 505. SCRAMBLING OF SEXUALLY EXPLICIT ADULT VIDEO SERVICE PROGRAMMING.**

(a) REQUIREMENT.—Part IV of title VI (47 U.S.C. 551 et seq.), as amended by this Act, is further amended by adding at the end the following:

47 USC 561.

**"SEC. 641. SCRAMBLING OF SEXUALLY EXPLICIT ADULT VIDEO SERVICE PROGRAMMING.**

"(a) REQUIREMENT.—In providing sexually explicit adult programming or other programming that is indecent on any channel of its service primarily dedicated to sexually-oriented programming, a multichannel video programming distributor shall fully scramble or otherwise fully block the video and audio portion of such channel so that one not a subscriber to such channel or programming does not receive it.

Children and youth.

"(b) IMPLEMENTATION.—Until a multichannel video programming distributor complies with the requirement set forth in subsection (a), the distributor shall limit the access of children to the programming referred to in that subsection by not providing such programming during the hours of the day (as determined by the Commission) when a significant number of children are likely to view it.

"(c) DEFINITION.—As used in this section, the term 'scramble' means to rearrange the content of the signal of the programming so that the programming cannot be viewed or heard in an understandable manner.".

47 USC 561 note.

(b) EFFECTIVE DATE.—The amendment made by subsection (a) shall take effect 30 days after the date of enactment of this Act.

**SEC. 506. CABLE OPERATOR REFUSAL TO CARRY CERTAIN PROGRAMS.**

(a) PUBLIC, EDUCATIONAL, AND GOVERNMENTAL CHANNELS.—Section 611(e) (47 U.S.C. 531(e)) is amended by inserting before the period the following: ", except a cable operator may refuse to transmit any public access program or portion of a public access program which contains obscenity, indecency, or nudity".

(b) CABLE CHANNELS FOR COMMERCIAL USE.—Section 612(c)(2) (47 U.S.C. 532(c)(2)) is amended by striking "an operator" and inserting "a cable operator may refuse to transmit any leased access program or portion of a leased access program which contains obscenity, indecency, or nudity and".

**SEC. 507. CLARIFICATION OF CURRENT LAWS REGARDING COMMUNICATION OF OBSCENE MATERIALS THROUGH THE USE OF COMPUTERS.**

(a) IMPORTATION OR TRANSPORTATION.—Section 1462 of title 18, United States Code, is amended—

(1) in the first undesignated paragraph, by inserting "or interactive computer service (as defined in section 230(e)(2) of the Communications Act of 1934)" after "carrier"; and

(2) in the second undesignated paragraph—

(A) by inserting "or receives," after "takes";

(B) by inserting "or interactive computer service (as defined in section 230(e)(2) of the Communications Act of 1934)" after "common carrier"; and

(C) by inserting "or importation" after "carriage".

(b) TRANSPORTATION FOR PURPOSES OF SALE OR DISTRIBUTION.—The first undesignated paragraph of section 1465 of title 18, United States Code, is amended—

(1) by striking "transports in" and inserting "transports or travels in, or uses a facility or means of,";

(2) by inserting "or an interactive computer service (as defined in section 230(e)(2) of the Communications Act of 1934) in or affecting such commerce" after "foreign commerce" the first place it appears;

(3) by striking ", or knowingly travels in" and all that follows through "obscene material in interstate or foreign commerce," and inserting "of".

(c) INTERPRETATION.—The amendments made by this section are clarifying and shall not be interpreted to limit or repeal any prohibition contained in sections 1462 and 1465 of title 18, United States Code, before such amendment, under the rule established in United States v. Alpers, 338 U.S. 680 (1950). 18 USC 1462 note.

**SEC. 508. COERCION AND ENTICEMENT OF MINORS.**

Section 2422 of title 18, United States Code, is amended—

(1) by inserting "(a)" before "Whoever knowingly"; and

(2) by adding at the end the following:

"(b) Whoever, using any facility or means of interstate or foreign commerce, including the mail, or within the special maritime and territorial jurisdiction of the United States, knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years to engage in prostitution or any sexual act for which any person may be criminally prosecuted, or attempts to do so, shall be fined under this title or imprisoned not more than 10 years, or both.".

**SEC. 509. ONLINE FAMILY EMPOWERMENT.**

Title II of the Communications Act of 1934 (47 U.S.C. 201 et seq.) is amended by adding at the end the following new section:

**"SEC. 230. PROTECTION FOR PRIVATE BLOCKING AND SCREENING OF OFFENSIVE MATERIAL.** 47 USC 230.

"(a) FINDINGS.—The Congress finds the following:

"(1) The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.

"(2) These services offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops.

"(3) The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.

"(4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.

"(5) Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.

"(b) POLICY.—It is the policy of the United States—

"(1) to promote the continued development of the Internet and other interactive computer services and other interactive media;

"(2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;

"(3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;

"(4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and

"(5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

"(c) PROTECTION FOR 'GOOD SAMARITAN' BLOCKING AND SCREENING OF OFFENSIVE MATERIAL.—

"(1) TREATMENT OF PUBLISHER OR SPEAKER.—No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

"(2) CIVIL LIABILITY.—No provider or user of an interactive computer service shall be held liable on account of—

"(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

"(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

"(d) EFFECT ON OTHER LAWS.—

"(1) NO EFFECT ON CRIMINAL LAW.—Nothing in this section shall be construed to impair the enforcement of section 223 of this Act, chapter 71 (relating to obscenity) or 110 (relating

to sexual exploitation of children) of title 18, United States Code, or any other Federal criminal statute.

"(2) NO EFFECT ON INTELLECTUAL PROPERTY LAW.—Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.

"(3) STATE LAW.—Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.

"(4) NO EFFECT ON COMMUNICATIONS PRIVACY LAW.—Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986 or any of the amendments made by such Act, or any similar State law.

"(e) DEFINITIONS.—As used in this section:

"(1) INTERNET.—The term 'Internet' means the international computer network of both Federal and non-Federal interoperable packet switched data networks.

"(2) INTERACTIVE COMPUTER SERVICE.—The term 'interactive computer service' means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

"(3) INFORMATION CONTENT PROVIDER.—The term 'information content provider' means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.

"(4) ACCESS SOFTWARE PROVIDER.—The term 'access software provider' means a provider of software (including client or server software), or enabling tools that do any one or more of the following:

"(A) filter, screen, allow, or disallow content;

"(B) pick, choose, analyze, or digest content; or

"(C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.".

## Subtitle B—Violence

### SEC. 551. PARENTAL CHOICE IN TELEVISION PROGRAMMING.

47 USC 303 note.

(a) FINDINGS.—The Congress makes the following findings:

(1) Television influences children's perception of the values and behavior that are common and acceptable in society.

(2) Television station operators, cable television system operators, and video programmers should follow practices in connection with video programming that take into consideration that television broadcast and cable programming has established a uniquely pervasive presence in the lives of American children.

(3) The average American child is exposed to 25 hours of television each week and some children are exposed to as much as 11 hours of television a day.